INDUSTRISPIONASJE
OG ARBEIDSGIVERS KONTROLLADGANG MOT INDUSTRISPIONASJE

Kandidatnr: 419
Veileder: Henning Jakhelln
Leveringsfrist: 25.11.03

Til sammen 17 619 ord

13.01.2004

Innholdsfortegnelse

1 Innledning

1.1 Tema og problemstilling

I denne oppgaven skal jeg se på begrepet industrispionasje, hva det innebærer og hvordan det forekommer. Deretter vil jeg vurdere hva arbeidstaker kan gjøre for å beskytte seg mot at bedriften blir utsatt for industrispionasje.

Retten til å utføre et arbeid er nedfelt i en rekke internasjonale konvensjoner slik som EMK[1] og SP[2], og kommer også til uttrykk i vår egen Grunnlov § 110(1)[3]. Mennesker trenger sitt arbeide, både for sin egen utfoldelses skyld, og ikke minst for å tjene til livets opphold. I et hvert arbeidsforhold vil vi ha en arbeidsgiver og en arbeidstaker. Til grunn for dette forholdet vil det ligge et gjensidig lojalitetsforhold. Arbeidsforholdet vil ikke kunne eksistere uten en nødvendig eksisterende tillitt mellom arbeidsgiver og arbeidstaker. Svikter de ansatte blir bedriften sårbar. Industrispionasje er kanskje det ultimale tillitsbrudd, da arbeidstakers handlinger vil kunne medføre enorme konsekvenser for både arbeidsgiver og de andre ansatte fordi bedriften kan miste hele sitt eksistensgrunnlag på grunn av slikt svik. Industrispionasje er ikke bare et alvorlig tillitsbrudd, det er også straffebelagt etter straffeloven[4] § 294 nr 2 og 3 og § 405a.

1.2 Avgrensning av oppgaven

I denne oppgaven er det begrepet industrispionasje som skal behandles. Det vil ikke være plass for en nøye drøftelse og vurdering av de eksisterende lovreglene mot slik spionasje, men jeg vil gi en kort gjennomgang av disse.

---

[1] Den Europeiske Menneskerettskonvensjon, 1950

[2] Konvensjon om Sivile og Politiske rettigheter, 1966

[3] Grunnloven av 1814, om retten til arbeide

[4] Lov av 22.mai Nr.10. 1902, Almindelig borgerlig Straffelov. (Heretter forkortet til strl.)

Videre er det industrispionasje innenfor næringslivet som skal vurderes, og jeg avgrenser derfor mot militæretterretning. Spionasje mot militæret i et land er et område som vill falle utenfor de naturlige grensene for denne oppgaven, da det er bedriftene og arbeidsgiverne i næringslivet sitt forsvar mot industrispionasje det skal skrives om.

En annen avgrensning må gjøres mot problematikken rundt konkurranse med tidligere arbeidsgiver. Dette er et tema som fort kan streife innom industrispionasje, da en del av det å forsvare seg mot konkurranse fra tidligere arbeidstakere nettopp går ut på at de ikke skal bruke bedriftshemmeligheter de har fått kunnskap om fra det tidligere ansettelsesforholdet. Dette er likevel ikke et område jeg har mulighet til å gå innpå, da det vil bli på siden av min hovedproblemstilling.

Jeg skal i denne oppgaven se på arbeidsgivers adgang til å igangsette kontrolltiltak mot industrispionasje. Det er mange ulike typer kontrolltiltak som kan være effektive og nødvendige i arbeidslivet. Men jeg har i denne oppgaven ikke mulighet til å vurdere adgangen til kontroll i arbeidslivet generelt,[5] men skal kun se på kontrolltiltak som kan verne mot industrispionasje.
En problemstilling som er direkte relatert til kontrolltiltak er behandling av personopplysninger og lovreglene rundt dette som fremgår av personopplysningsloven. Jeg skal som sagt ikke skrive om kontrolltiltak generelt, og det er begrenset hvor mye personopplysningsloven vil spille inn ved de kontrolltiltakene som her skal vurderes. Jeg er likevel nødt til å behandle reglene fra personopplysningsloven der dette er naturlig for oppgavens sammenheng, men noen inngående vurdering av loven er det ikke mulighet for.

1.3 Oppbygning av oppgaven

I det følgende vil jeg forsøke å definere begrepet industrispionasje og tegne et bilde av hvorfor dette er en alvorlig trussel for enhver bedrift som forsøker å holde stand i et hardt konkurranse preget marked. Så vil jeg gå inn på hva en arbeidsgiver kan gjøre for

[5] For mer om generelle former for kontroll i arbeidslivet, se Underutvalgets rapport til Arbeidslivslovutvalget, 2002.

å forhindre at industrispionasje forekommer i hans bedrift. I den forbindelse må vi se på grunnlaget for arbeidsgiverskontrolladgang før jeg tar for meg de ulike kontrolltiltak som kan igangsettes for å forhindre industrispionasje. Disse tiltakene vil bli drøftet ut fra arbeidsgivers behov for kontroll opp mot arbeidstakers behov for integritet.

2 Industrispionasje

2.1 Definisjon av industrispionasje

Det finnes ingen helt klar definisjon av ”industrispionasje”. Andre uttrykk som blir brukt er for eksempel forretningsspionasje, handelsspionasje, økonomisk spionasje, bedriftsspionasje, markedsspionasje. I noen land brukes uttrykket ”illojal konkurranse”, og enkelte forsøker kanskje til og med å legalisere overtredelsen ved å kalle det ”aggressiv markedsundersøkelse”. Ordet industrispionasje er likevel det mest dekkende for den type spionasje det her er snakk om, da det ikke snevrer inn begrepet for mye. Ved å bruke begrepet industrispionasje i stedet for noen av de andre begrepene, sørger man for at både det private og det offentlige næringslivet inkluderes.
Jeg mener at ordet industrispionasje er et bedre og mer dekkende ord, og det er også det ordet som jeg tror er mest innarbeidet i den språklige forståelse.
Jeg vil i det følgende forsøke å gi en nærmere definisjon og forklaring av hva industrispionasje innebærer.

Industrispionasje vil si at en person klarer å få tak i en bedriftshemmelighet på en illojal eller uetisk måte. Denne personen kan være en av de ansatte i den bedriften det begås lovbrudd mot som så videreformidler bedriftshemmeligheten videre. Men det kan også være en helt utenforstående person som på en eller annen måte klarere å skaffe seg tilgang til bedriften og dens hemmeligheter. Det kan dreie seg om spionasje internt i Norge mellom to konkurrerende bedrifter, eller det kan være en utenlandsk bedrift eller til og med utenlandsk etterretning som forsøker å få tak i en bedriftshemmelighet. Jeg vil ikke skille mellom disse formene da spionasjen uansett vil foregå etter det samme mønsteret hvor målet er det samme; å få tak i en hemmelighet. Når jeg bruker uttrykket ”industrispionasje” i denne oppgaven er det derfor ment som et fellesbegrep for de ulike formene for spionasje mot en bedrift som kan oppstå.

2.1.1 Lojalitetskravet

Det å bevare en bedriftshemmelighet når du er ansatt i en bedrift vil si det samme som å holde på en hemmelighet. Arbeidsgiver er nødt til å kunne stole på at de ansatte er lojale og ikke utleverer hemmeligheter. Det rettslige utgangspunktet er at det gjelder en alminnelig, ulovfestet lojalitetsplikt i et arbeidsforhold. [6] Industrispionasje er det ultimale troskapsbrudd fra en ansatt, en krenkelse av alt det lojalitetsplikten innebærer.

Lojalitetsplikt vil si "troskapsplikt" både mot arbeidsgiver og mot arbeidskamerater, og innebærer at den ansatte ikke skal foreta handlinger som kan skade foretaket. Det skal eksistere et nødvendig nivå av tillitt mellom arbeidsgiver og den ansatte. Det er ikke bare den ansatte som skal være lojal, det påligger også arbeidsgiver å utvise lojalitet overfor sine ansatte. Arbeidsgiver utviser lojalitet ved å sørge for at de ansatte har et arbeid å gå til, at en vil få arbeidsoppgaver å utføre, at de nødvendige sikkerhetstiltak er tatt på arbeidsplassen og ikke minst at arbeidstaker får utbetalt lønn for sin arbeidsprestasjon. Kort sagt at arbeidstaker vil bli behandler ordentlig. Arbeidstaker vil utvise sin lojalitet ved å være punktlig, utfører gitte oppgaver, ikke være borte fra arbeidet uten gyldig fravær og ikke minst, at arbeidstaker ikke stjeler fra arbeidsgiver eller setter arbeidsgivers bedrift i fare ved ulojale handlinger. Arbeidsgiver er med andre ord i en langt mer utsatt posisjon for illojalitet enn arbeidstaker og det er derfor stilt svært strenge krav til lojalitet i arbeidsforhold. Arbeidsmiljøloven[7] § 66(1) omhandler bestemmelsene om avskjed. Her går det klart frem at arbeidstaker må øyeblikkelig fratre stillingen sin hvis han/hun har gjort seg skyldig i "grovt pliktbrudd eller annet vesentlig mislighold av arbeidsavtalen". Illojalitet kan altså slås hardt ned på med de alvorligste følger for arbeidstaker.

Når arbeidsgiver ansetter en person er det for å få visse arbeidsoppgaver utført. Arbeidsforholdet kan da medføre at den ansatte er nødt til å få innsyn og kunnskap om bedriftshemmeligheter. Men det er lojalitetsforholdet, eller tillitsforholdet til den ansatte som må ligge til grunn for at arbeidsgiver i det hele tatt skal tørre å la en ansatt få innsyn i dennes bedriftshemmeligheter.

---

[6] Se bla. Rt. 1996 s. 1401, Rt. 1990 s. 607 og Rt. 1993 s. 300.

[7] Lov om arbeidervern og arbeidsmiljø m.v. av 4. feb. nr. 4 1977, heretter forkortet aml.

Lojalitetsplikten innebærer at det er visse begrensninger om hva den ansatte kan omtale både internt i bedriften med andre kollegaer, eksternt til familie og venner, og ikke minst i forhold til offentligheten og pressen. Men dette vil jeg ikke gå nærmere inn på her da jeg skal holde meg til "den harde kjerne" av hva som er beskyttelsesverdig i forhold til virksomhetens eksistens. Bedriftshemmeligheter er typisk en del av denne kjernen, og den ansatte vil ut fra lojalitetsplikten være pålagt taushetsplikt om bedriftshemmelighetene. Problematisering i forhold til når en arbeidstaker allikevel må kunne røpe en hemmelighet går jeg ikke nærmer innpå her. Dette vil bli drøftet nærmere under punkt 4.3 og 4.4 om taushetsplikt og taushetserklæringer.

2.2 Bedriftshemmeligheter

Jeg har til nå snakket om begrepet bedriftshemmelighet som om dette er et allment kjent og brukt uttrykk. Fullt så enkelt er det ikke. Ordet bedriftshemmelighet er udefinert i norsk rett og har vært et omdiskutert begrep. Jeg vil i det følgende derfor forsøke å vise hva begrepet bedriftshemmelighet innebærer ved hjelp av ulike rettskilder.

2.2.1 Definisjon av bedriftshemmeligheter

I Bokmålsordboka[8] er den normale språklige forståelsen av ordet "hemmelig" definert som noe "som bare er kjent av én eller av en liten innvidd krets".
"Hemmelighet" defineres som "det å være skjult for uinnvidde", og "noe som er eller bør være hemmelig". Ut fra ordbokdefinisjonen kan hemmeligheter sies å være informasjon om noens anliggender som ønskes holdt hemmelig for resten av omverdenen. Men hva er da en bedriftshemmelighet? Er dette en form for hemmeligheter som skiller seg fra den normale forståelsen av ordet?

På det nordiske juristmøtet i 1934 var Ragnar Knoph en av deltakerne. Et av temaene som var oppe til diskusjon var rettsbeskyttelsen av bedriftshemmeligheter, noe Knoph var særlig opptatt av. Han hadde i forkant av møtet skrevet en avhandling",[9] og det var denne som dannet grunnlaget for diskusjonen på møtet den første dagen. Man diskuterte den daværende lovgivningen som fantes for bedriftshemmeligheter og rettsbeskyttelsen av disse. Ingen av landene hadde en egen lov om bedriftshemmeligheter, en del av

[8] Bokmålsordboka, 1986

landene hadde regler spredt rundt i lovverket og ingen hadde en definisjon av begrepet. Dette var noe Knoph mente var en mangel ved systemet og inviterte derfor til debatt om emnet.

Knoph definerte bedriftshemmeligheter på Nordisk Juristmøte i 1934 slik:

> ” Med en bedriftshemmelighet forstår man innsikter og kunnskaper som en forretning eller en fabrikk har, og som man holder hemmelig for selv å kunne utnytte dem i kampen mot konkurrentene”.[10]

Knoph nevner videre eksempler på hva som kan sies å være slik innsikter og kunnskaper, herunder fabrikkhemmeligheter som nye metoder, gammel oppskrift, oppfinnelse man ikke har patent på, gunstig innkjøpssted, en god salgsorganisasjon, kundelister osv. Knoph skriver i sin avhandling at det kan diskuteres om ordet bedriftshemmelighet er det mest dekkende ordet eller det ordet som språklig sett er å foretrekke. Strl. § 294 nr. 2 omtaler det for eksempel som ”driftshemmelighet” eller ”forretningshemmelighet”. Men som Knoph sier:

> ”Det er i alle fall fullt forsvarlig å bruke ordet bedriftshemmelighet som et overbegrep som omfatter alle hemmeligheter innenfor erhvervslivet”.[11]

Vi har fortsatt ingen lovbestemt definisjon av ”bedriftshemmelighet”. I 1972 fikk vi en ny lov om markedsføring,[12] og i denne lovens paragraf 7 ble det inntatt en bestemmelse om bedriftshemmeligheter. Begrepet bedriftshemmeligheter blir drøftet i disse forarbeidene og vi bør se nærmere på disse for å få et klarer bilde av begrepet. Men før vi ser nærmere på forarbeidene, kan det være lurt å se på bakgrunnen for at den nye loven kom til i 1972.

2.2.2 Historikk

På jurist møtet i 1934 etterlyste Knoph klarere regler på området og advarte mot utviklingen innen næringslivet som ble stadig mer konkurransepreget. I en presset situasjon er det klart at visse mennesker tar i bruk ufine metoder for å få en fordel på markede. Industrispionasje kan medføre enorme tap for den bedriften det går utover. I 1934 nevner Knoph at en tysk industrimann hadde regnet ut at bare i et enkelt år hadde

---

[9] Knoph, 1934

[10] Forhandlinger på det 16. Nordiske Juristmøte, 1934

[11] Knoph, 1934

[12] Lov om kontroll med markedsføring og avtalevilkår av 16.juni nr.47. 1972 (heretter forkortet mfl.)

Tyskland tapt 800 millioner mark på grunn av spionasje fra utlandet.[13] Slike tap er et land nødt til å beskytte seg mot, og Tyskland hadde rettspraksis etter hvert utviklet et relativt vidt begrep om hva industrispionasje innebar.

I Norge hadde vi lov om illojal konkurranse fra 1922. Men det var ikke i denne loven en fant noe om bedriftshemmeligheter, den hadde bare en bestemmelse om misbruk av betrodde tegninger og lignende. Bestemmelsen om bedriftshemmeligheter var å finne i strl. § 294 nr 2[14]. Danmark hadde lov om "Bestemmelser mod uretmæssig Konkurrence og Varebetegnelse". Svenskene hadde sin "Lag av 29.mai 1931 med vissa bestämmelser mot illojal konkurrens" og Finland hadde "Lag om illojal konkurrens". Men ingen av disse lovene hadde en definisjon av begrepet bedriftshemmelighet. Dette så Knoph som et problem da han mente at lovgiverne ikke

> "har søkt å se bedriftshemmelighetenes problem i øinene i hele dets sammenheng, men har operert fra fall til fall, nærmest efter et skipperskjønn"[15]

Knoph etterlyste en klar lov om bedriftshemmeligheter med en dertil definisjon av begrepet. I Norge verserte på dette tidspunktet Hydro saken[16] som gjaldt uaktsom industrispionasje, og det var i den forbindelse reist krav om skjerping av reglene om bedriftshemmeligheter. Knoph mente det ville være nyttig med klarere regler på området for å kunne bekjempe fenomenet bedre.

I 1966 ble det levert en innstilling fra Konkurranselovkomiteen[17] om forslag til en ny konkurranse lov hvor man også ville ha en egne regler for bedriftshemmeligheter. Det ble påpekt at det manglet en klar bestemmelse som rammet bedriftsspionen som kommer utenfra. Man brukte den gang generalklausulen i den daværende loven for å ramme slike tilfeller. Komiteen kom med forslag om å fjerne bestemmelsen i strl. § 294 nr. 2, og heller ha alle bestemmelser vedrørende bedriftshemmeligheter samlet i en lov. Komiteen mente at det ikke var nødvendig å innta en definisjon av begrepet, men viste til Knoph sin definisjon av begrepet i avhandlingen han skrev til det allerede omtalte juristmøtet av 1934.

---

[13] Forhandlinger på det 16. nordiske jurist møtet, 1934

[14] Hvor den fortsatt står i dag, dog noe endret

[15] Knoph, 1934

[16] Rt 1937 s.62

[17] Innstilling fra konkurranselovkomiteen, om ny konkurranselov, 1966 (endte som markedsføringsloven)

Behandlingen av den nye loven ble til en Odelstingsproposisjon[18]. Her heter det ikke lenger Konkurranselov, men lov om markedsmisbruk. Kort sammenfattet blir det her sagt at komiteen har kommet med mange gode forslag, men man ser ikke nødvendigheten av en egen lov om konkurranse med et eget kapittel for bedriftshemmeligheter. Man vil heller fortsette som før med § 294 nr. 2 i straffeloven og heller legge til et ledd i denne, og i tillegg gi en helt ny bestemmelse[19] for å favne opp de tilfellene som ikke klart ble rammet den gangen. Videre skulle det være en bestemmelse om bedriftshemmeligheter i den nye loven om markedsmisbruk. Departementet mener at denne bestemmelsene ikke trenger å være fullt så omfattende som komiteen ville ha den.
I Innstilling til Odelstinget[20] henger man seg på forslagene fra Odelstingsproposisjonen, men mener at regelen om bedriftshemmelighet som skal inn i den nye loven kun skal omfatte næringslivet siden det gjelder en lov om markedsmisbruk. Resultatet er Lov av 16.juni 1972 nr. 47, Lov om kontroll med markedsføring.

Situasjonen i dag er ikke så annerledes enn den i 1934. Vi har fortsatt ingen definisjon av begrepet bedriftshemmeligheter og lovgivningen er spredt i forskjellige lover.

2.3 Forarbeidene til markedsføringsloven av 1972

Både Innstillingen fra konkurranselovkomiteen og den påfølgende Odelstingsproposisjonen og Innstillingen til Odelstinget fastslår at det ikke finnes definisjon av begrepet i verken norsk eller fremmed lovgiving. Likevel besluttet man å ikke gi en definisjon av bedriftshemmeligheter, men det blir uttalt en del rundt begrepet i Innstillingen fra konkurranselovkomiteen som blir tilsluttet av Odelstingsproposisjonen og Innstillingen til Odelstinget.[21] Jeg vil i det følgende forsøke å gi en kort oversikt over hva som ble sagt og vektlagt rundt begrepet bedriftshemmeligheter fra lovgivers side i 1972.

---

[18] Odelstings proposisjon nr. 57, Lov om markedsmisbruk, 1971-72 (markedsføringsloven)

[19] Dette resulterte i strl. § 405 a

[20] Innstilling Odelstinget XIX, Lov om kontroll med markedsføring, 1971-72 (markedsføringsloven)

[21] Ot.prp. nr.57 1971 -72

2.3.1 Forarbeidenes kriterier for en bedriftshemmelighet

I Innstilling fra konkurranselovkomiteen vises det for det første til at begrepet "bedriftshemmelighet" har blitt tatt opp i språket etter Knoph innførte det som begrep på juristmøtet i 1934, og komiteen slutter seg til dette begrepet. Komiteen tar så for seg trekk som de mener er beskrivende for bedriftshemmeligheter. I korthet ble det vektlagt: De alminnelige kunnskaper og erfaringer som en ansatt får under sin ansettelse er ikke å betrakte som bedriftshemmeligheter. Videre kreves det at det foreligger viten som er spesifikk for vedkommende bedrift, og som er av betydning for deres virksomhet. Komiteen mener at arbeid med produktutvikling og prøver med nye varetyper kan være bedriftshemmelighet. Det kan også driftsresultater og statistikker, likså planer for markedsføring, tidspunkt for visse innsatser i reklame m.v., innkjøpskilder for råstoffer m.v.

2.3.2 Forarbeidenes kriterier for hemmeligholdelse

Komiteen oppstiller så noen krav til bedriften om hemmeligholdelse for at de skal ha rett til beskyttelse etter loven:
For det første må bedriften uttrykkelig ha markert kravet på hemmeligholdelse, eller dette må ligge klart i selve situasjonen. Det er videre ikke nødvendig at bare en enkelt bedrift eller forretning har hemmeligheten, den er hemmelig selv om bedriften inngår for eksempel lisensavtaler og lignende. Det foreligger en hemmelighet selv om flere innen bedriften kjenner den[22] , men det må være en begrensning slik at det ikke oppstår usikkerhet rundt varig hemmeligholdelse. Komiteen oppstiller heller ikke noe krav om at hemmeligheten må være absolutt ny. Det henvises her til Knoph[23] sin avhandling hvor det blir sagt at gammel viten som "gjenoppdages" eller "gjenoppfinnes" kan være en bedriftshemmelighet. Eller det kan tenkes at to uavhengige bedrifter kommer frem til en metode som hver av dem beholder som hemmelig.

Komiteen kommer også med noen uttalelser rundt "know-how" begrepet og avgrensninger rundt dette i forhold til bedriftshemmeligheter. "Know-how" dekker gjerne hovedsaklig området mellom bedriftshemmeligheter og almen teknisk viten. Det er derfor en flytende grense mellom disse to uttrykkene. I denne oppgaven har jeg ikke

[22] Komiteen viser her til Skeie, strafferett II, s.495

[23] Knoph, 1934

mulighet til å gå inn på en gjennomgang og drøftelse av "know-how" problematikken. For mer om dette, se Innstillingen fra Konkurranselovkomiteen s.48 ff.

Kort oppsummert kan en si at forarbeidene vektlegger to hovedkrav til bedriftshemmeligheter. De må være beskyttelsesverdig, altså dreie seg om viten det er av interesse for bedriften å holde hemmelig. Dessuten må det også sies å foreligge en hemmelighet, herunder at bedriften faktisk har klart å hindre at andre har fått kjennskap til hemmeligheten.

2.4 Andre rettskilder

Jeg har til nå brukt juridisk litteratur og forarbeider for å finne en definisjon av bedriftshemmeligheter. Mye av det komiteen legger vekt på i forarbeidene er trukket ut fra Knoph sin avhandling fra 1934. Men lovgiver ser likevel bort fra Knoph sin anbefaling om å ha en definisjon av begrepet for å unngå uklarheter og dermed søke å forhindre gråsonetilfelle. Slik sett må en nok dessverre konstantere at begrepet derfor forblir uavklart og omdiskutabelt.

I vårt naboland Sverige har man derimot gitt en lovebestemt definisjon av bedriftshemmeligheter. I 1990 fikk man etter lang tids arbeide en egen lov om "skydd för företagshemligheter". Loven er kort og konsis og man har ikke bare en definisjon av begrepet bedriftshemmelighet, eller "företagshemlighet" som det heter på svensk, men man har også inntatt regler om når noe ikke kan sies å være et angrep på en bedriftshemmelighet. Det kan derfor ha meget for seg å ta en nærmere titt på denne loven og jeg vil i punktet under forsøke å gi en oversikt over hva man har kommet frem til i Sverige.

2.4.1 Den svenske loven om "skydd av företagshemligheter"[24]

I lovens § 1 defineres begrepet bedriftshemmeligheter og hva som skal forstås med dette slik:

> "Med företagshemligheter avses i denna lag sådan information om affärs- eller driftförhållanden i en näringsidkares rörelse som näringsidkaren håller hemlig och vars röjande är ägnat att medföra skada för honom i konkurranshänseende.

[24] Lag om skydd för företagshemmelighetr, av 1.juli 1990, Sverige

> Med information förstås både sådana uppgifter som har dokumentats i någon form, inbegripet ritningar, modeller och andra liknande tekniska förebilder, och enskilda personers kännedom om ett visst förehållande, även om det inte har dokumenterats på något särskilt sätt."

Man har valgt å gi ordet bedriftshemmeligheter en meget vid betydning. Slik det beskrives her vil det omfatte ett hvert internt forhold i bedriften som holdes hemmelig, både skriftlig og muntlig, og som kan påvirke dennes konkurranseevne.
Leser man denne bestemmelsen isolert vil det virke som om loven gir beskyttelse til et hvert forhold en bedrift ønsker å skjule for allmennheten. Lovgiver ønsket derimot ikke å gi beskyttelse til ulovlig eller klandreverdig oppførsel i en bedrift, og gav derfor en nærmere spesifisering av hva som skulle regnes som urettmessige angrep mot en bedrift i lovens § 2, som vi snart skal se nærmer på. Det vil da dreie seg om en hemmelighet som bedriften ønsker å holde skjult, men det vil ikke være en bedriftshemmelighet i ordets rette forstand.

Denne loven beskytter næringsdrivende som driver en eller annen form for virksomhet. Kravet om hemmeligholdelse er ikke absolutt, personer som trenger informasjonen for å utføre sitt arbeide må kunne få denne uten at det da slutter å være en bedriftshemmelighet. Men det kreves at den krets som har tilgang til informasjonen lar seg avgrense og definere. Et annet krav er at den næringsdrivende faktisk holder informasjonen hemmelig. Det skal finnes et ønske eller et formål fra den næringsdrivendes side om at bedriftshemmeligheten det er snakk om ikke spres utenfor en viss krets av personer.

Så langt ser vi at denne loven har mange av de samme elementene som fremgår av de norske forarbeidene til markedsføringsloven. Grunnen til dette kan ligge i at man startet arbeidet med markedsloven etter det hadde vært en lovrevisjon med de nordiske komiteer, hvor man var enige om at de gjeldende bestemmelsene ikke var tilfredsstillende, og man arbeidet seg frem mot et lovforslag som i hovedsaken var innholdsmessig like. [25] I Sverige har man likevel endt opp med å samle reglene om bedriftshemmeligheter i en lov til forskjell fra de andre nordiske landene. Men den

[25] Ot.prp. nr.57 1971-72

svenske loven setter også opp noen grenser for hva som kan sies å være en bedriftshemmelighet.

2.4.2 Skydd för företagshemligheter § 2

Hemmeligheter bedriften har som at de for eksempel bruker helsefarlig fremstillingsmetoder eller at de driver med heleri er ikke bedriftshemmeligheter som fortjener beskyttelse. Når man i § 1 første ledd bruker uttrykket "medföra skada för honom i konkurranshänseende" mener man skade i konkurransehenseende som en domstol i en rettssak i prinsippet skal kunne tilkjenne erstatning for, noe man ikke vil kunne gjøre når det er begått lovbrudd.[26]

Lovens § 2 sier:

> " Lagen gäller endast obehöriga angrepp på företagshemligheter.
>
> Som ett obehörigt angrepp anses inte att någon anskaffar, utnyttjar eller röjer en företagshemlighet hos en näringsidkare för att offentliggöra eller inför en myndighet eller annat behörigt organ avslöja något som skäligen kan misstänkas utgöra brott, på vilket fängelse kan följa, eller som kan anses utgöra annat allvarligt missförhållande i näringsidkarens rörelse.

Lovbrudd som kan medføre fengsel beskyttes ikke, og videre rammer man andre svært alvorlige forhold i en bedrift, som for eksempel miljøkriminalitet, selv om denne ikke er ulovlig ved uttrykket "annat allvarligt missförhållande". Loven er her ikke uttømmende, den nevner bare de viktigste situasjonene. Det er tre kriterier som må være oppfylt for at det ikke skal være utilbørlig å anskaffe, utnytte eller røpe en bedriftshemmelighet.[27]

For der første må noen anskaffe, utnytte eller røpe en bedriftshemmelighet.

For den andre må dette skje for å avsløre noe. Man må så se på hensikten bak å avsløre hemmeligheten. Det må ikke være snakk om noen form for økonomisk vinning. Den som velger å avsløre en bedriftshemmelighet bør forsøk å handle slik at handlingen viser at formålet objektivt har vært at allmennheten skal bli gjort kjent med forholdet.

Og for det tredje kreves det at hemmeligheten som offentliggjøres må gjelde et forhold som gir skjellig grunn til mistanke om et lovbrudd som kan medføre fengselsstraff, eller som kan anses utgjøre annet alvorlig missforhold i den næringsdrivendes bedrift. Det er

---

[26] Iseskog, 1990,

[27] jf. Iseskog, 1990,

altså ikke en hvilken som helst hemmelighet som kan avsløres, den må være av en viss alvorlig karakter.[28]

2.4.3 Er norsk rett samsvarende med den svenske?

De norske forarbeidene er også inne på de samme vurderingsfaktorer som den svenske loven oppstiller, men ikke like utførlig. Konkurranselovkomiteen gir en vurdering av hvorfor bedriftshemmeligheter skal eller bør ha et særlig vern, men understreker

> ” Det at det foreligger en hemmelighet og at bedriften har søkt å bevare den, kan derfor ikke i og for seg – alene – være tilstrekkelig til å gi beskyttelse overfor tredjemann.”[29]

De konkluderer derfor med at det foreligger ikke et vern bare fordi det foreligger en bedriftshemmelighet, men sier at kravet må være at hemmeligheten blir søkt utnyttet av en konkurrent ved hjelp av forkastelige midler. Det er altså det utilbørlige angrepet som skal være straffebelagt og denne tankegangen bifalles av departementet. [30] Dette samsvarer godt med den svenske lovens bestemmelse i § 2 som sier ” Lagen gäller endast obehöriga angrepp på företagshemligheter”, og en må kunne anta at noe av den samme tankegangen om at forbrytelser eller andre svært klandreverdige forhold ikke fortjener lovs beskyttelse. Men det ingenting i de norske lovbestemmelsene eller forarbeidene som fanger opp det den svenske lovgivningens bestemmeleser om når det er tillatelig å offentliggjøre en bedriftshemmelighet. Dette har vist seg å kunne være problematisk i forholde til trykkefriheten og ytringsfriheten særlig i forhold til forsvarshemmeligheter, og vi bør derfor se nærmer på denne problemstillingen.

2.5 Industrispionasje og ytringsfriheten

Utgangspunktet er Grunnlovens § 100 siste punktum om ytringsfrihet med mulighet for lovebestemte grenser for denne friheten. Utgangspunktet er full ytringsfrihet, det er begrensningene i ytringsfriheten som trenger nøye begrunnelse. Ytringsfriheten kan begrenses ved ærekrenkelser, men Høyesterett har hatt en tendens til å tolke bestemmelsen her forholdsvis fritt. Videre kan det settes grenser til vern for svake grupper i samfunnet, slik som for eksempel minoritetsgrupper av ulik etnisk bakgrunn eller homofile og lesbiske. Også her viser høyesterettspraksis at det har blitt lagt stor

---

[28] jf. Iseskog, 1990

[29] Innstilling fra konkurranselovkomiteen, 1966

[30] se Ot.prp. nr. 57 1971-72

vekt på prinsippet om full ytringsfrihet. En siste grense går mot ytringer om forsvaret og da særlig militærtjenesten. Her har derimot Høyesterett vist liten vilje til å tolke straffebestemmelsene rundt dette innskrenkende på grunnlag av ytringsfrihetens prinsipp, og personer har for eksempel blitt idømt straff for oppfordring til militærnekting.

2.5.1 Ikkevold saken

En av de mest kjente sakene rundt ytringsfrihet og forsvarsforhold er den såkalte "Ikkevold" saken fra 1986[31]. En gruppe som var imot krig og militærtjeneste på generelt grunnlag bestemte seg for å samle informasjon om forsvarsforhold på Andøya hvor de mente Norge hadde et seismisk system for registrering av ubåter. De brukte offentlig tilgjengelige midler som telefonkatalogen, offentlige navnelister fra forsvaret og feltturer hvor de tok bilder. Det samlede materiale resulterte i noen artikler hvor de blant annet konkluderte med at et slik ubåt registreringsradar var på Andøya. Ingen hadde fortalt dem dette, det var ren spekulasjon fra deres side basert på det ellers innsamlede materialet. Forsvaret anmeldte dem på denne bakgrunn og det ble tatt ut tiltale mot gruppen. Forsvaret mente at opplysninger som ikke var ment for allmennheten, altså forsvarshemmeligheter, var blitt utlevert og det utgjorde en fare i forhold til fremmede stater. [32]

Spørsmålet som oppstår her er meget interessant. Gruppen hadde jo nemmelig ikke fått tak i opplysninger som var hemmeligholdt, eller samlet opplysninger på noen lovstridig måte. Det de hadde gjort, var å legge sammen de opplysningene de fikk tak i via offentlig registre og lignende, og på den måten lagt sammen to og to og konkludert med hvor dette hemmelige anlegget måtte ligge. Spørsmålet blir jo da, hva er egentlig en hemmelighet? De offentlige opplysningene var ikke hemmelige og fotografiene de tok var ikke tatt på ulovlig vis. Så hvor går grensen mellom det å få tak i noe som er hemmelig, og det å bruke tilgjengelige opplysninger til å kalkulere seg frem til en hemmelighet? Problemstillingen kan lett oppstå i forhold til industrispionasje. Driver man spionasje ved å samle inn all den informasjon man kan få fatt i, eller er det bare uskyldig informasjonsundersøking?

---

[31] Rt. 1986 s. 536

[32] Jakhelln, 1987 og Jakhelln, 1990

2.5.2 Når er noe en hemmelighet?

En tysk etterretningsmann har fortalt at han var på oppdrag i Norge før annen verdenskrig brøt ut. Han tok inn på et hotell i Oslo hvor han så rolig og systematisk jobbet seg gjennom telefonkatalogen. Ut fra denne offentlig tilgjengelige kilden fikk han flere interessante opplysninger han så kunne rapportere hjem til Tyskland. Ved å foreta denne undersøkningen i Norge vekket han heller ingen mistanke og han kunne også få flere opplysninger ved å oppsøke bedriftene hvor han kun ved å presentere seg som tysk forretningsmann ble gitt kataloger, brosjyrer, årsregnskaper osv.[33] Alt dette er offentlig tilgjengelig informasjon som alle kunne få tak i. Likevel var det han gjorde spionasje. Men hvorfor? Er det da kanskje formålet vi må se på?

I den tidligere nevnte "Ikkevold"-saken, gjorde de jo akkurat det samme, men med en meget vesentlig forskjell. Hele poenget med de undersøkelsene de foretok seg var nettopp å publisere det, gjøre det kjent for allmennheten som de mente hadde en rett til disse opplysningene. De ønsket å bruke sin ytringsfrihet til å starte en offentlig debatt, og det må jo sies å være en beskyttelses verdig rett?
Når det gjelder industrispionasje, enten det være seg mot et annet land eller din argeste konkurrent, så er hele poenget å gjøre det i skjul. Altså å sørge for at verken bedriften det spioneres mot, eller noen andre finner ut hva som foregår. Og det vil dessuten bli gjort i en vinnings hensikt. Om det er å skaffe seg en ny teknologi eller vite hvor konkurrenten står, så vil det være snakk om økonomisk gevinst. Ofte vil denne gevinsten være betydelig. Det vil ikke være noe ønske om å benytte sin ytringsfrihet i slike tilfeller.
I forhold til forsvaret vil det være strengere grenser mot ytringsfriheten. Spørsmålet er bare når denne grensen er overtrådt og hva det er den ønsker å beskytte. Det er ikke nødvendig å slå ned på en hvilken som helst overtredelse. Det er i det øyeblikket landets sikkerhet settes på spill at det er grunn til å slå ned på det.

2.6 Ulike former for industrispionasje

Vi har nå sett at det kan problematisk å fastslå om noe er spionasje eller kun ytringer. La oss derfor i det følgende se på hva de ulike formene for spionasje kan være.

---

[33] Heradstveit, 1976

2.6.1 Aktsom industrispionasje

Det klassiske eksemplet er den aktsomme spionasjen som er utført i fullt overlegg. Dette kan foregå på forskjellige måte, det kan typisk være overlevering av papirer av forskjellig slag, annenhånds informasjon og bilder. Etter hvert som teknologien har utviklet seg har vi fått mer avanserte former som avlytting, overvåking, lyd- og videoopptak, e-post og ikke minst "hacking" inn i datasystemer til bedriften for å ødelegge eller for å hente ut informasjon. Ved overlagt industrispionasje vil det ofte være en ansatt i bedriften som utfører udåden, men det kan også være en utenforstående som har klart å få adgang til bedriften enten på lovlig eller ulovlig vis. Dette dreier seg om en form for organisert spionasje og overtredelsen er et bevisst angrep på en bedrift.

Et eksempel på slik overlagt industrispionasje fremgår av Hydro saken fra 1937.[34] Forholdet som var oppe til avgjørelse i Høyesterett i 1937 dreide seg riktignok om uaktsom industrispionasje av Dr. Blich, men mannen som fikk ham til å begå denne udåden bedrev en meget planlagt form for spionasje. Dr. Collett hadde sluttet i Hydro, men drev fortsatt i samme bransje. Men det viste seg i ettertid at han over lengre tid hadde samlet informasjon om Hydro på forskjellig vis. Da politiet undersøkte leiligheten hans fant de både tekniske tegninger fra Hydro, og en mappe som het Dr. Blich. I denne mappen hadde Collett samlet informasjon om Hydro som han hadde lurt ut av Blich. Dr. Collett hadde drevet en meget omfattende spionasje mot Hydro, og saken rystet Norge da den verserte i 1930 årene.

2.6.2 Uaktsom industrispionasje

I den andre enden av skalaen har vi den uforsettlige, uforsiktige eller uaktsomme industrispionasjen. Denne formen er kanskje den farligste for en bedrift, da overtrederen som regel ikke vil være klar over at han begår denne handlingen og dermed er det vanskelig å forhindre at slike handlinger forekommer. Men hvis en person ikke er klar over at han eller hun begår industrispionasje, hvordan skal arbeidsgiver da klare å forhindre dette?

Når industrispionasjen er uaktsom beveger vi oss over i en gråsone hvor vi er mer inne på det personlige planet i et arbeidsforhold enn det rent tekniske. Det vil her være snakk

[34] Rt. 1937 s.62

om å kontrollere oppførselen til den ansatte i stedet for kontroll av arbeidsplassen. Det kan være lett å tro at uaktsom industrispionasje ikke forekommer så ofte, eller at situasjonen i seg selv er så spesiell at man kan i det minste ikke klandre den ansatte. Men saken er nok heller den at uaktsom industrispionasje nok er noe som forekommer daglig i arbeidslivet, folk snakker rett og slett for mye. Den uaktsomme industrispionasjen dreier seg ofte om hvor grensen går mellom det som må regnes som fortrolig snakk mellom kollegaer, ektefeller og venner, til det som må regnes som overlevering av informasjon til utenforstående. Et godt eksempel på slik uaktsom industrispionasje er den tidligere omtalte høyesterettsdommen fra 1937 side 62.

2.6.3 Hydro dommen og andre eksempler på uaktsomhet

Det antas her at en ingeniør, Dr. Blich, gjennom samtaler med sin venn og tidligere arbeidskollega, Dr. Collet, hadde røpet bedriftshemmeligheter. Dr. Blich var ikke klar over at Collett bedrev industrispionasje mot Hydro, og hadde en egen mappe med navnet ”dr. Blich” hvor han samlet opplysninger han fikk. Dr. Blich var bundet av taushetserklæringer fra Hydro, og det var ingen tvil om at han hadde brutt disse og Hydro var berettiget til å avskjedige ham. Hydro nøyde seg derimot ikke bare med å avskjedige Blich, men foretok en del andre tiltak for blant annet å sett et eksempel til advarsel for de andre funksjonærene. Spørsmålet var om Hydro var berettiget til dette, eller om de hadde gått for langt. Høyesterett kom frem til at avskjedigelsen var berettiget, men at man gikk for langt når man satte opp plakater på selskapets oppslagstavler som informerte de andre ansatte om at dr. Blich var avskjediget på grunn av ”kontraktsbrudd”, da dette var med på å bygge opp under de allerede eksisterende ryktene om at Blich hadde vært med å konspirere mot Hydro, noe han ikke hadde.

Rt 1937 side 62 viser hvordan uaktsom industrispionasje lett kan ramme selv den mest aktsomme bedrift. Hydro hadde foretatt seg flere ting for å forhindre at det inntrufne skulle skje. I tillegg til sikkerhetstiltakene rundt Hydro, påla kontrakten mellom Hydro og dr. Blich ham hemmeligholdelse og generaldirektør Aubert hadde videre personlig forbudt ham å omtale visse forhold. Det kan være nyttig med et eksempel til for å illustrere hvor lett uaktsom industrispionasje kan forekomme.

En ansatt i en bedrift (A) har for eksempel vært i et møte med en annen bedrift (B) for å representere de nye modellene som A’s bedrift ønsker å tilby denne bedriften. På vei

hjem kommer den ansatte i snakk med en hyggelig mann (X), og det viser seg at de jobber innen samme felt. Det faller seg derfor naturlig at de begynner å diskutere arbeidet sitt og bedriftene de jobber i. Ikke et øyeblikk faller det A inn at denne hyggelige fremmede kan være en representant for et konkurrerende firma som gjennom samtalen dem i mellom kan skaffe seg en rekke nyttige opplysninger om firmaet, salgsplaner eller til og med teknikk de holder på å utvikle.

2.7 Lovreglene til beskyttelse mot industrispionasje

Jeg vil i dette avsnittet se nærmere på de eksisterende lovreglene som gjelder bedriftshemmeligheter og som er aktuelle for problemstillingen i denne oppgaven. Om dette er gode, klare regler skal ikke vurderes her, det følgende vil kun være en kort gjennomgang og forklaring av det gjeldende lovverket på området.
Det finnes også andre bestemmelser som gjelder bedriftshemmeligheter slik som straffeprosessloven[35] § 124 (1) og tvistemålsloven[36] § 209 (1) som gjelder et vitnes rett til å nekte å besvare spørsmål hvis det medfører at forretnings- eller bedriftshemmelighet avsløres. Videre kan det nevnes at patentloven[37] § 2 (5) nr 1 gir en mulighet til å få patent på en oppfinnelse selv om den har blitt kjent hvis det skyldes "åpenbart misbruk" i forhold til søkeren eller noen denne utleder sin rett fra. Det må da skje innen seks måneder. Jeg kommer ikke til å gå inn på disse reglene da jeg i denne oppgaven skal vurdere situasjonen rundt spionasje mot bedrifter, og problemstillingene rundt disse nevnte reglene faller derfor naturlig utenfor rammen av min oppgave.
Som nevnt før er den aktuelle lovgivningen spredt. De aktuelle reglene for denne oppgaven blir å finne i to forskjellige kapitler i straffeloven og markedsføringsloven.

2.7.1 Straffeloven § 294 nr. 2

Etter sin rettslige plassering hører denne bestemmelsen inn under forbrytelser om "skadeverk". Denne bestemmelsen kom til etter Tyskland i 1896 fikk sin lov om illojal konkurranse. I 1922 fikk også Norge sin egen lov om illojal konkurranse, men man valgte å ikke flytte denne bestemmelsen fra straffeloven og over i den nye loven, enda

[35] Lov om rettergangsmåten i straffesaker av 22.mai 1981 nr. 25

[36] Lov om rettergangsmåten for tvistemål av 13. aug. 1915 nr. 6

[37] Lov om patenter av 15.des. 1967 nr. 9

det sies rett ut i forarbeidene til § 294 nr. 2 at den er et utslag av den tyske lovens bestemmelser.
Bestemmelsen rammer den som ”uberettiget enten selv gjør Brug af en Forretnings- eller Driftshemmelighet” som tilhører en bedrift denne jobber for eller har jobbet for de siste 2 årene eller i løpet av de to siste årene ”har havt Del” i, eller ”aabenbarer en saadan i Hensigt å sætte en anden i stand til å gjøre Brug af den, eller som ved Forledelse eller Tilskyndelse medvirker hertil”.
§ 294 nr.2 ramme arbeidstaker som slutter i en bedrift og som så vil gjøre bruk av hemmeligheter denne har fått kunnskap om gjennom ansettelsesforholdet. Bestemmelsen tar her altså sikte på å gi beskyttelse til hemmeligheter etter et arbeidsforhold har tatt slutt, men det blir satt en tidsbegrensning på to år. Videre rammes medeiere eller ansatte som åpenbarer en bedriftshemmelighet når hensikten er at en annen skal kunne gjøre bruk av den. Bestemmelsen rammer derimot ikke en spion som kommer utenfra og som på umoralsk vis skaffer seg kunnskap om en bedriftshemmelighet og utnytter den, og heller ikke den som tar i bruk en hemmelighet som er oppdaget på denne måten.
Strafferammen er bøter eller fengsel i inntil 6 måneder.

2.7.2 Straffeloven § 294 nr. 3

Bestemmelsen rammer den som ”uberettiget gjør bruk av en bedrifts forretnings- eller bedriftshemmelighet”, når man har fått kunnskap eller rådighet over denne ved å ha vært teknisk eller merkantil konsulent for bedriften eller hatt et oppdrag fra den. Bestemmelsen rammer også konsulenter som ”uberettiget åpenbarer en slik hemmelighet” for å sette andre i stand til å gjøre bruk av den, eller som ”ved forledelse eller tilskynding medvirker til dette”.
§ 294 nr.3 kom til i 1972 etter arbeidet med markedsføringsloven for å fange opp tilfeller hvor konsulenter jobber for en bedrift og derigjennom får tilgang til bedriftshemmeligheter. Ikke bare direkte bruk av en hemmelighet rammes, men også det å sette en annen i stand til å bruke en slik hemmelighet. Medvirkning er også straffbart.
Strafferammen er også her bøter eller fengsel i opptil 6 måneder.

2.7.3 Straffeloven § 405

Denne paragrafen ble lagt til for å fange opp tilfeller med spionen utenfra som det manglet en bestemmelse om. Bestemmelsen er å finne under i straffelovens 40de kapittel om ”Forseelser mod Formuesrettigheder”.
§ 405 a rammer den som på ”urimelig måte skaffer seg eller søker å skaffe seg kunnskap om eller rådighet over en bedriftshemmelighet”. Den vil typisk ramme spioner utenfra, men også en bedrifts tjeneste- eller tillitsmann som uberettiget benytter eller setter andre i stand til å benytte bedriftens hemmeligheter.
Strafferammen er her bøter eller fengsel i 3 måneder.

2.7.4 Markedsføringsloven § 7

Som nevnt over kom markedsloven til etter en lovrevisjon var foretatt som fastslo at gjeldende rett på området ikke var tilfredsstillende nok. Man la til grunn at det var behov for en egen regel som vernet bedriftshemmeligheter i den nye markedsloven, da man ønsket å gå beskyttelse til investeringene og det harde arbeidet som en næringsdrivende har nedlagt.
§ 7 retter seg derfor mot den næringsdrivende og de som opptrer på hans vegne.
Det er to tilfeller av misbruk bestemmelsen typisk kan ramme:
For det første hvor overtrederen har fått kunnskap om eller rådighet over hemmeligheten på grunn av enten et tjenesteforhold, et tillitserverv eller et forretningsforhold,(§ 7 første ledd), og for det andre at noen har fått kunnskap eller rådighet over en bedriftshemmelighet fordi noen har brutt taushetsplikten eller foretatt annen rettstridig handling, (§ 7 andre ledd).

3 Arbeidsgivers adgang til kontroll

3.1 Innledning

I dagens samfunn hvor konkurransen mellom de næringsdrivende blir hardere og hardere, fremtrer behovet for å kunne beskytte seg mot illojal konkurranse eller spionasje mot sin bedrift som et nødvendig overlevelsesvilkår.
Som kunde har vi utallige valgmuligheter. Er man ikke fornøyd med et produkt eller en tjeneste bytter man simpelthen merke eller leverandør. De næringsdrivende kan derfor

sies å ha større press på seg enn noen gang til å ligge et hakk foran sine konkurrenter og makte å tilby det lille ekstra som gjør at de beholder sine gamle kunder og eventuelt skaffer seg noen nye. Det sier seg selv at man da får et behov for å beskytte seg mot enhver trussel som kan virke ødeleggende på ens konkurranseevne. Dette inkluderer både ansatte i egen bedrift, konkurrenter og andre som av forskjellige årsaker har tilgang til firmaet. En bedriftseier som vet konkurrentene er ute etter dennes bedriftshemmeligheter vil selvsagt føle et enormt behov for å beskytte sine interesser. Særlig med tanke på at åpenbaring av bedriftshemmeligheten kan innebære både økonomisk tap og tap av konkurranseevne for bedriften, noe som igjen kan føre til bedriftens undergang og at de ansatte mister jobbene sine. Bedriftseieren vil derfor være interessert i å igangsette ulike kontrolltiltak for å forhindre at spionasje forekommer. Men hvilken rett har arbeidsgiver til å igangsette slike tiltak?

3.2 Grunnlaget for kontroll

Norsk rett har ingen generelle regler om hvilke kontrolltiltak som kan iverksettes overfor arbeidssøkere og ansatte. Reglene følger dels av de alminnelige regler om rettigheter og plikter i arbeidsforholdet, og dels av lovfestede og ulovfestede regler om vern av personlig integritet. Allmenne rettsprinsipper, lov, tariffavtaler og rettspraksis setter opp grenser for kontrolladgangen. Jeg vil i her gi en kort oversikt over disse grunnlagene.

3.2.1 Styringsretten

Arbeidsgivers mulighet til å igangsette kontroll av de ansatte er en del av arbeidsgivers styringsrett. Styringsretten innebærer arbeidsgivers adgang til å lede, fordele og kontrollere arbeidet. Styringsretten er ikke lovfestet men oppstår som en følge av inngåelsen av en arbeidsavtale. Rettspraksis fra Arbeidsretten slår fast at styringsretten gir grunnlag for å iverksette ulike kontrolltiltak.[38] I utgangspunktet er det også arbeidsgiver som bestemmer hvilke type kontrolltiltak som skal igangsettes og utformingen av disse, men det kan foreligge visse begrensninger for eksempel på grunnlag av tariffavtale.

[38] Rettspraksis bli behandlet i kapittel 4 om mulige kontrolltiltak

3.2.2 Samtykke

Muligheten for kontrolltiltak kan også stamme fra samtykke fra den eller de ansatte det gjelder i form av en individuell eller kollektiv avtale. Det stilles forholdsvis høye krav til samtykke. Det kreves at den ansatte har fullt ut forstått hva denne samtykker i, herunder rekevidden av kontrolltiltaket. Samtykke til den ansatte må være klart og enstydig. Et moment som spiller inn ved vurderingen av samtykke vil være tiltakets inngripende karakter. Hvor mer inngripende tiltaket er, jo strengere krav stilles til samtykke. Samtykke kan gis ved inngåelsen av arbeidsavtalen, (ansettelsen), eller etter ansettelsesforholdet er etablert og eventuelt i forbindelse med et konkret kontrolltiltak. Vanligvis er et samtykke noe man kan kalle tilbake, men man kan antagelig gjennom arbeidsavtalen gjøre samtykke ugjenkallelig for en kortere eller lengre periode forutsatt at det ikke er snakk om et tiltak av en så inngripende karakter at det berører frihet, ære eller legemets integritet som for eksempel narkotika- og alkoholtesting.

3.2.3 Andre grunnlag

Man kan også finne grunnlag for kontrolladgang i lov og forskrifter og kollektive avtaler. Arbeidsmiljøloven med forskrifter har for eksempel bestemmelser om et fullt forsvarlig arbeidsmiljø. Arbeidsgiver er pålagt å iverksette tiltak for å sikre dette.

Det må kunne tenkes at en tariffavtale danner grunnlag for bindende avtale om kontrolltiltak for de ansatte som er medlemmer av den foreningen det er inngått tariffavtale med. Medlemskapet i foreningen gir i utgangspunktet fullmakt til foreningen til å inngå avtaler om kontroll på arbeidsplassen, og vanligvis vil det være en rettferdig og forsvarlig saksgang og interesseavveining som ligger til grunn for den inngåtte avtalen. En grense bør likevel trekkes ved særlig inngripende kontrolltiltak som nevnt i punktet over, og det bør her forlanges et individuelt samtykke.

3.3 Grenser for kontrolladgang

Arbeidsgiver har altså full mulighet til å igangsette kontrolltiltak. Men som vi har sett over vil det være visse grenser for både tiltaket og hvordan arbeidsgiver går frem for å igangsette tiltaket. Arbeidsretten har gjennom flere avgjørelser satt opp rammer for adgangen til kontroll fra arbeidsgivers side. Det er arbeidsgivers behov for kontroll som må avveis mot de ansattes behov for vern av den personlige integritet.

Ut fra tidligere avgjørelser av Arbeidsrette kan arbeidstaker utføre kontroll av arbeidstiden, hvordan arbeidstiden anvendes, kontroll av utførelsen av arbeid og bedriftens omsetning.[39] Videre finnes det særlig tre sentrale dommer fra Arbeidsretten hvor kriteriene som retten legger til grunn ved vurderingen av et kontrolltiltak kommer frem. Jeg kommer ikke til å behandle dommene inngående her. Dette vil bli gjort i kapittelet om mulige kontrolltiltak arbeidsgiver vil igangsette mot industrispionasje.[40]

I ARD 1951 s. 201 gjaldt personkontroll av de ansatte ved inn- og utpassering fra bedriften. Alle de ansatte måtte trykke på en knapp som enten lyste rødt eller grønt. Kontrollen fungerte slik at det ikke var noen spesielle personer som var valgt ut. Kontrollen var også nedfelt i tariffavtale mellom arbeidsgiverforeningen og de ansattes forbund. I ARD 1978 s. 110 omhandler en bedrift som bedrev stikkprøve kontroll av de ansattes private kjøretøyer. Arbeidsretten viste her til en rekke tidligere avgjørelser som fastslår arbeidsgivers adgang til kontroll. Så uttaler retten at vilkåret for en slik adgang til kontroll er et saklig behov for tiltaket og at det ikke praktiseres vilkårlig ved å sette noen i en særstilling. Tilslutt uttales det at for at tiltaket skal være tariffrettslig holdbart må informasjons- og drøftelsesplikten etter Hovedavtalen være oppfylt. I den siste dommen, ARD 1959 s. 1, dreide det seg om inn- og utstempling skulle foretas i arbeidstøy eller ikke. Arbeidsgiver begrunnet pålegget om å utføre kontrolltiltaket i arbeidstøy med effektivitetshensyn. Arbeidsretten presiserte her at arbeidsgiver ikke kan pålegge kontrolltiltak som går utover andre og utenforliggende formål, eller som i utrengsmål griper inn i fritiden til de ansatte.

3.4 Kriterier som blir vektlagt i Arbeidsrettens praksis

Ut fra disse dommene kan vi trekke ut kriterier om saklighet, vilkårlighet og uforholdsmessige ulemper.

---

[39] Om Stemplingsur se ARD 1918-19 s.233, ARD 1950 s. 16, ARD 1958 s.19, ARD 1968 s.44, hyppighet av kontrollen se ARD 1940 s. 17.

[40] Se særlig punkt 4.5

3.4.1 Saklighet

For det første må tiltaket være basert på at det saklig sett er behov for tiltaket. Dette innebærer i følge ARD 1978 s. 110 at tiltaket ikke er åpenbart grunnløst eller motivert i utenforliggende hensyn.
En bedrift har for eksempel oppdaget mye svinn i sin produksjon som har ført til et økonomisk tap for bedriften. Bedriften vil her ha et reelt behov for å innføre et kontrolltiltak for å forhindre videre svinn. I en bedrift som ikke har problemer med svinn, vil det for eksempel være langt mer usikkert om man kan i gangsette slik kontroll kun på bakgrunn av en statistisk fare for svinn.

3.4.2 Vilkårlighet

Videre må tiltaket ikke praktiseres vilkårlig. Enkelte arbeidsgrupper må ikke settes i en særstilling uten en reell begrunnelse. De må ikke få verken bedre eller dårligere vilkår enn andre grupper, slik det går frem av ARD 1951s. 201 hvor alle var underlagt kontroll, og som forutsatt i ARD 1978 s. 110.
For å ta eksemplet mitt over, bedriften setter i gang et kontrolltiltak for å forhindre svinn i produksjonen, for eksempel veskekontroll. Så lenge de inkluderer alle de ansatte i kontrolltiltaket og ikke bare kontrollerer en utvalgt gruppe, for eksempel lagerarbeiderne, er ikke tiltaket vilkårlig.

3.4.3 Ulemper

For det tredje må ikke kontrollen etter sin karakter påføre arbeidstakerne så store ulemper at kontrollen av den grunn bli tariffrettslig angripelig, jf. ARD 1978 s. 110. Det må det ikke gis tiltak som går utover, eller er åpenbart uegnet til å fremme formålet med kontrolltiltaket eller som i utrengsmål griper inn i fritiden til de ansatte, som i ARD 1959 s. 1.
En vesentlig ulempe kan være at tiltaket medfører helsefare for de ansatte. Denne begrensningen vil nå også følge av aml. § 12 nr 1 som gjelder tilrettelegging av arbeidet. Her fremgår det bl.a. at arbeidstakerne ikke skal ”utsettes for uheldige fysiske eller psykiske belastninger…”.

3.5 Tariffavtaler

Vi finner videre grunnlag for kontroll i tariffavtaler. Adgangen til kontroll er regulert i flere hovedavtaler. Den mest sentrale er kanskje Hovedavtalen mellom LO og NHO med Tilleggsavtale V "Avtale om kontrolltiltak i bedriften".
Hovedavtalen LO-NHO § 9-13 nr.2 fastsetter at behov, utforming og innføring av interne kontrolltiltak skal drøftes på bedriften og at fungerende kontrolltiltak skal vurderes med jevne mellomrom. Denne bestemmelsen suppleres av Tilleggsavtale V. Punkt en og to i Tilleggsavtalen fastsetter:

> "1. Kontrolltiltak kan ha sitt grunnlag i teknologiske, økonomiske, sikkerhets- og helsemessige omstendigheter, samt andre sosiale og organisatoriske forhold i bedriften. Tiltak som innføres skal ikke gå ut over det omfang som er nødvendig og må være saklig begrunnet i den enkelte bedrifts virksomhet og behov."

> "2. Alle ansatte eller grupper av ansatte skal stilles likt i forhold til den kontroll som gjennomføres i henhold til punkt 1."

Det som går frem av disse to punktene må sies å være i samsvar med det som har kommet frem gjennom Arbeidsrettens avgjørelser, og disse bestemmelsene må derfor også kunne legges til grunn utenfor det området hvor Hovedavtalens bestemmeleser direkte gjelder.[41]

Hovedavtalen LO-NHO § 9-13 nr 3 gjelder fjernsynsovervåking av de ansatte. Det sies her at slik overvåking må være saklig begrunnet ut fra hensynet til virksomhet til bedriften som skal drive overvåking. Ved direkte og kontinuerlig overvåking av de ansatte skal hensikt og behov kartlegges, og det sies at slik overvåking i størst mulig grad bør unngås. Det vises tilslutt til personopplysningsloven med gjeldende forskrifter.

3.6 Personopplysningsloven[42]

Fjernsynsovervåking som kontrolltiltak reiser egne problemstillinger i forhold til personopplysningsloven. Jeg vil i det følgende kort gå innpå bestemmelsene i den

[41] Se Artikkelsamling i arbeidsrett, 2001, (Jakhelln "Om arbeidsgivers kontrolladgang")

[42] For en mer inngående redegjørelse av personopplysningslovens regler og virkeområde se bl.a. Wiik Johansen mfl. 2001, og Underutvalgets rapport, 2002

relativt nye Personopplysningsloven[43] av april 2000 som overtok for den tidligere lov om personregistre av 1978. Den nye Personopplysningsloven trådte i kraft 1. januar 2001. Loven ble vedtatt for å gjennomføre kravene i EUs personverndirektiv. Loven gjelder for behandling av personopplysninger på alle samfunnsområder, herunder arbeidslivet. Noe som betyr at hvis et kontrolltiltak innebærer en behandling av personopplysninger, vil personopplysningsloven avgjøre denne siden av kontrolltiltakets gyldighet. Loven gir uttømmende bestemmelser om adgangen til videoovervåking.

Lovens § 1 fastslår at formålet med loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger og at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn som personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.

Lovens virkeområde defineres i § 3. Loven omfatter de kontrolltiltak som innebærer behandling av personopplysninger i en eller annen form. I utgangspunktet vil da andre kontrolltiltak som blodprøvetaking, narkotikatesting, brevåpning og lignende falle utenfor. Disse tiltakene vil omfattes av vernet av den personlige integritet etter menneskerettighetene og ulovfestede arbeidsrettslige prinsipper som vi har vært inne på i punktene over. All elektronisk behandling av personopplysninger omfattes av loven, jf. § 3 litra a. Litra b bestemmer at manuell behandling omfattes dersom det skal tas inn i et register.

Reglene om fjernsynsovervåkning er særskilt omhandlet i kapittel VII i loven.
Med fjernsynsovervåking menes vedvarende eller regelmessig gjentatt personovervåking ved hjelp av fjernbetent eller automatisk virkende kamera, fotografiapparat eller lignende apparat, jf. popplyl. § 36. Paragraf 37 som bestemmer virkeområdet for loven slår fast at særreglene i dette kapittelet gjelder ”all fjernsynsovervåking”. Det slås videre fast at reglene i §§ 8,9 og 11 om formålsangivelse, opplysningskvalitet og meldeplikt også skal gjelde all fjernsynsovervåking. Men det er verdt å merke seg at lovgiver ikke ønsket å beholde de

[43] Heretter forkortet til popplyl.

samme strenge kravene til å drive fjernsynsovervåking som i den gamle loven[44], når formålet med overvåkingen er å avdekke kriminell adferd, se § 2 nr. 8 b. Paragraf 37 sier derfor at kravene til særskilt grunnlag for å behandle sensitive opplysninger ikke skal gjelde, men de alminnelige kravene etter § 8 må likevel være oppfylt.

Paragraf 38 gir grunnkravene for overvåking. Det fremgår videre i § 38 at fjernsynsovervåking bare er tillatt dersom det ut fra virksomheten er et særskilt behov for dette. Denne bestemmelsen er en videreføring av personregisterlovens § 37 a, som hadde et krav om "saklig behov". Hva som må forstås med "særskilt behov" må vurderes i vær enkelt situasjon. I forarbeidene til personregisterloven § 37 a er det uttalt at kravet var oppfylt hvis for eksempel en bedrift ønsket å foreta overvåking som en del av arbeidet med å forebygge at farlige situasjoner oppstår, eller av hensynet til sikkerheten til da ansatte eller andre.[45]

Paragraf 40 gjelder varsel om at overvåking finner sted. Denne bestemmelsen er en videreføring av den tidligere § 390 b i straffeloven, men til forskjell fra denne bestemmelsen gjelder popplyl. § 40 også områder hvor en begrenset krets av personer ferdes jevnlig.
Det skal varsles når overvåking finner sted og varslet skal være tydelig. På offentlig sted gjøres dette enklest med skilting. I overvåkingssituasjoner som gjelder sted hvor en begrenset krets av personer ferdes, for eksempel i en arbeidssituasjon, vil det være mer hensiktsmessig og informere om tiltaket på en annen måte.

3.7 Avgjørelser om overvåking av de ansatte

Vi så tidligere at Arbeidsretten har åpnet for en relativt vid mulighet for arbeidsgiver til kontrolladgang, så fremt kriteriene om saklighet, vilkårlighet og ulemper er oppfylt. Disse kriteriene hviler på hensynene til arbeidsgivers rett til kontroll opp mot arbeidstakers rett til integritet. De samme hensynene ligger bak de alminnelige prinsipper om personvern. Beskyttelsen av arbeidstakeres personvern har vært oppe i

[44] Den tidligere lov av 9.juni 1978 nr. 48 om personregistre

[45] Odelstingsproposisjon nr. 56, 1992-93, Om lov om endring i lov 9.juni 1978 nr 48 om personregistre m.m.

Høyesterett flere ganger. Jeg behandler ikke dommene inngående i dette punktet, da det vil bli gjort under punkt 4 om kontrolltiltak for å forhindre industrispionasje.

Som det fremgår av punkt 3.6 vil den nye personopplysningsloven gi uttømmende regler om adgangen til videoovervåking. Tidligere rettspraksis er likevel viktig fordi den gir gode eksempler på interesseavveiningen som retten skal foreta etter de ulovfestede prinsippene om kontroll i arbeidsforhold. Det er særlig to kjente høyesterettsdommer som fastslår rammene for arbeidsgivers rett til kontroll kontra arbeidstakers rett til integritet. Rt. 1991 s. 616 og Rt. 2001 s. 668 gjelder begge hemmelig videoovervåkning, hvor arbeidsgiver startet overvåking av de ansatte for å bevise mulig illojalitet. I begge sakene legger Høyesterett til grunn at de ulovfestede regler om personvern tilsier at hemmelig videoopptak ikke vil kunne bli ført som bevis verken i arbeidsrettssaker eller straffesaker. Det understrekes at slike opptak er sterkt personvern krenkende, og bør derfor ikke forekomme. Avgjørelsene stemmer godt overens med den linjen man har lagt seg på internasjonalt.
Det finnes også andre dommer om andre typer kontrolltiltak. Rt. 2001 s. 1589 gjaldt blant annet kontroll av loggen til internettbruken i bedriften. Bedriften fikk her medhold i at de foretatte tiltakene var i overensstemmelse med reglene om personvern. I RG 1993 s. 77 hadde arbeidsgiver gått inn på den ansattes private brukerområdet i bedriftens databaserte postsystem. Her fant retten at arbeidsgiver ikke hadde lov til å gå inn på dette området.

Det går frem av avgjørelsene om kontrolltiltak at domstolene vektlegger kontrolltiltakets saklighet og forholdsmessighet. I tillegg ses det på saksbehandlingen forut for kontrolltiltaket, informasjon og drøftelser er for eksempel særskilt viktig. Det går også frem at den som skal utsettes for kontrolltiltaket som regel vil ha rett på informasjon om tiltaket. Disse elementene er de samme som gikk frem Arbeidsrettens praksis om kriterier for kontrolltiltak, og videre det som fremgår av tariffavtalen mellom LO og NHO.[46]

[46] Se punkt 3.5

4 Aktuelle kontrolltiltak for å forhindre industrispionasje

4.1 Innledning

Denne oppgaven dreier seg om industrispionasje og jeg kommer som presisert i kapittel 1 ikke til å ta for meg et hvert tenkelig kontrolltiltak i en arbeidssituasjon.

Ved kontrolltiltak har vi nå konstatert at det er to ulike interesser som kolliderer. På den ene siden har vi arbeidsgivers behov for å sikre sine bedriftshemmeligheter og dermed sin bedrift, og på den annen side har vi den ansattes behov for vern av personlig integritet. Når jeg i det følgende skal drøfte og vurdere aktuelle kontrolltiltak mot industrispionasje er det disse to interessene og utredningene i punktene ovenfor som vil ligge til grunn for drøftelsene.

Når jeg nå skal gå gjennom ulike typer kontrolltiltak mot industrispionasje, vil jeg ha som utgangspunkt en bedrift som er avhengig av sine bedriftshemmeligheter og som derfor vil miste sin konkurranseevne hvis disse blir bekjentgjort.
Arbeidsgivers adgang og behov for å igangsette kontrolltiltak mot industrispionasje må avveies mot arbeidstakers rett til personvern. Det må kunne legges til grunn at kontrolltiltak for å forsvare seg mot industrispionasje er en saklig interesse. Spørsmålet blir om det er tiltak som likevel blir for omfattende og om ulempende ved det blir uforholdsmessige i forhold til personvernet til den ansatte.

4.2 Bakgrunnsjekk av den ansatte

Aml. § 55 A setter grenser for hvilke opplysninger en arbeidsgiver har adgang til å innhente i forbindelse med ansettelser. Det listes opp en rekke opplysninger som arbeidsgiver ikke har lov å spørre om eller innhente på andre måter, som for eksempel holdning til politiske, religiøse eller kulturelle spørsmål. Krav om slike opplysninger kan heller ikke tas inn i stillingsannonsen. Det gjøres unntak for forbudet hvis slike opplysninger er begrunnet i stillingens karakter eller hvis det inngår i formålet for virksomheten å fremme bestemte politiske, religiøse eller kulturelle syn og stillingen er av betydning for gjennomføringen av formålet. Det må i så fall opplyses i utlysningen av stillingen at slike opplysninger vil bli krevd av søkeren. Tilsvarende begrensninger følger av ILO konvensjon nr. 111 (1958), som er ratifisert av Norge.

En bedrift som skal beskytte seg mot industrispionasje, vil nok særlig være interessert i vandelen til en person som skal få tilgang til bedriften. Arbeidsgiver ønsker å forsikre seg mot at det ansettes noen som allerede har utvist illojalitet i sitt arbeide, og man ønsker derfor en nøye bakgrunnsjekk av den ansatte. Ut fra aml. § 55 A må bedriften trolig kunne stille spørsmål om søkeren er tidligere straffet, siktet eller er satt under tiltale for straffbare forhold hvis arbeidsgiver forutsetter uplettet vandel og dette har betydning for stillingen. Arbeidssøkeren har risikoen for å svare sannferdig.
Med hjemmel i strafferegistreringslovens § 10 er det gitt forskrift fra Justisdepartementet av 20.des 1974 nr. 4 om strafferegistrering. Av forskriftens § 12 går det frem at det som hovedregel ikke er adgang for arbeidsgiver å innhente politiattest. Unntaket gjelder for visse yrker innen for eksempel luftfart, farmasøytisk industri og for søkere til grunnskolen.[47] Arbeidsgiver kan neppe omgå bestemmelsen i forskriften § 12 ved å forlange at den ansatte eller arbeidssøkende, fremlegger opplysninger fra Strafferegisteret ved å benytte seg av sin egen rett til innsyn etter forskriften § 6.
I en bedrift hvor industrispionasje kan være særlig ødeleggende, vil man nok være berettiget til å i det minste spørre om søkerens vandel på dette og beslektede områder. Problemet er at man da er nødt til å sette sin lit til at søkeren svarer sannferdig på spørsmålet. Finner man ut i ettertid at søkeren ikke svarte sannferdig vil dette kunne være grunnlag for oppsigelse.

4.2.1 Bakgrunnsjekk av familie, nærstående, omgangskrets m.m.

En ting er om arbeidsgiver har adgang til å ta et inngående intervju med søkeren til stillingen, men hva med søkerens familie, venner og andre som denne omgås? Vil ikke de også kunne utgjøre en trussel?
Det kan ikke sies å foreligge noen form for rettslig grunnlag som tilsier at en arbeidsgiver skal ha rett og mulighet til å intervjue eller sjekke ut familien og andre som står søkeren nær. En mulighet er jo om søkeren blir spurt under intervjuet om noen i familien eller bekjentskapskretsen er tiltalt, siktet eller straffet for noen straffbare forhold. Om dette kan sies å være relevant for stillingen må sies å være heller tvilsomt, og mest sannsynlig vil arbeidsgiver ikke kunne stille et slikt spørsmål. Søkeren kan i

[47] Jf. Opplæringslova av 1998 nr.61, § 10-9, hvor det må fremgå av politiattesten at søkeren ikke er straffet, siktet eller tiltalt for seksuelle overgrep mot barn.

hvert fall ikke sies å være forpliktet til å svare. Det står riktignok ingenting i aml. § 55 A om forbud mot spørsmål om privatlivet til søkeren, men det må ut fra alminnelige ulovfestede prinsipper om privatlivets fred kunne antas at spørsmål av så privat karakter ikke har relevans for arbeidsforholdet, og derfor ikke er noe søkeren må stå til rette for. På den annen side må en ha forståelse for at en arbeidsgiver som skal forsvare sine bedriftshemmeligheter vil ha en interesse av å vite om søkerens nærmeste familiemedlemmer har vært straffet for industrispionasje. En kan riktignok ikke identifisere søkeren med sin nærmeste familie, men arbeidsgiver bør kanskje ha mulighet til å i det minste være klar over forholdet. I forbindelse med konkurranse med tidligere arbeidsgiver har problemstillingen om familiemedlem kan identifiseres med arbeidstaker vært oppe i Rt. 1996 s. 1401. Retten gikk ikke inn på spørsmålet da den fant at forholdet ikke hadde vært motiverende for saken. Men det utelukkes heller ikke. I teorien legges det til grunn at det skal "mye til" før en arbeidstaker og vedkommende nærstående må vurderes under ett.[48] Hvis det kan trekkes en parallell fra dette forholdet til denne oppgavens tema, blir spørsmålet om det å skulle beskytte sine bedriftshemmeligheter og herunder sin bedrifts overlevelse er nok til å si at nærstående bør kunne identifiseres med arbeidssøkeren.

4.3 Taushetsplikt

Til en viss grad kan det utledes en generell taushetsplikt av den alminnelige lojalitetsplikten[49] i et arbeidsforhold. Det vanligste er i dag at de fleste arbeidsavtaler inneholder en bestemmelse om taushetsplikt. Taushetsplikt vil si at den ansatte er forpliktet til å holde tett om, eller ikke snakke med andre om visse forhold i bedriften. I utgangspunktet gjelder taushetsplikten det den ansatte måtte få kjennskap til gjennom sitt arbeid slik som opplysninger og kunnskap om arbeidsstedet, arbeidsgivers person, og tekniske eller forskningsmessige opplysninger.
Taushetsplikten opphører ikke når arbeidsforholdet er avsluttet, og brudd på den vil medføre konsekvenser, se mfl. § 7 og strl. §§ 294 og 405 a.
Men noen ganger kan det reises spørsmål om hvor langt taushetsplikten til den ansatte strekker seg, om det er grenser for hva som kan bli pålagt å holdes tyst om og hvorvidt

[48] Fanebust, 1995.

[49] Se punkt 2.1.1 om lojalitetsplikten.

den ansatte kan gå til det offentlige eller media med forhold i bedriften som ønskes hemmeligholdt. Disse spørsmålene vil jeg behandle i punktene under, men først må vi se på taushetserklæringer som er en nærmere spesifikasjon av den generelle taushetsplikten.

4.4 Taushetserklæringer

Noen bedrifter vil ha noe mer enn den generelle taushetsplikten. Man ønsker med dette å understreke alvoret i det å holde tett om arbeidsforholdene, eller å definere et enda strengere område for hva som skal være taushetsbelagt. Det vanlige er da å bruke egne taushetserklæringer som spesifiserer nærmere hva det er den ansatte ikke skal snakke med uvedkommende om. Arbeidsgivers rett til å be den ansatte om å skrive under på en slik taushetserklæring må kunne utledes fra styringsretten til arbeidsgiver, og må ses på som en del av arbeidsavtalen partene imellom.

4.4.1 Kan den ansatte pålegges å underskrive taushetserklæring?

En annen ting er om den ansatte har mulighet til å nekte å skrive under på en slik erklæring om taushet. En må da se på den ansatte sine grunner for å nekte. Arbeidsgiver går for eksempel for langt i sine krav til den ansatte ved for eksempel å pålegge den ansatte om å tie om et straffbart forhold eller andre kritikkverdige forhold i bedriften. En bedrift kan ikke bruke en taushetserklæring for å forhindre at det offentlige tilsyn skal få vite om ulumskheter i bedriften. Her vil hensynet til det offentliges behov for å få vite hva som foregår veie tyngre enn konsekvensene det vil få for en bedrift at "hemmeligheten" deres blir røpet. Den ansatte må da ha rett til å nekte å skrive under på en slik taushetserklæring. Noen ganger har man ikke bare rett til å si fra, men også en plikt til å snakke ut om et forhold som ikke er bra i bedriften.

4.5 Begrense antallet som får tilgang til bedriftshemmelighetene

Arbeidsgiver vil ut fra styringsretten stå fritt til å fordele og lede arbeidsoppgavene. Arbeidsgiver må derfor fritt kunne bestemme hvem som skal jobbe og ha tilgang til bedriftshemmelighetene.[50] Jeg vil her komme med noen forslag til noen tiltak

[50] Se for øvrig punkt 3.2.1 om styringsretten

arbeidsgiver kan bruke for å begrense antallet ansatte som har tilgang til bedriftshemmelighetene.

4.5.1 Kopier og makulering

Et enkelt men viktig sikkerhetstiltak er å ikke oppbevare unødvendige kopier av bedriftshemmeligheten. Kopier og originaler som skal tas vare på må oppbevares på forsvarlig måte, hvordan man sikrer oppbevaringsstedene kommer jeg straks innpå i punktene under. Det er også viktig å ha sikre makulerings metoder, slik at ikke dokumenter med sensitiv informasjon kastes på en usikker måte slik at det kommer i feil hender.
Disse to enkle forhåndsreglene er enkle tiltak som ikke vil kollidere med personvernet til de ansatte, og arbeidsgiver må fritt kunne sette i gang slike tiltak.

4.5.2 Passord til data

Å sørge for at bare de innvidde har tilgang til filer og spesielle datamaskiner som inneholder informasjon om bedriftshemmelighetene, er et relativt enkelt tiltak som kan utføres for å hindre at uvedkommende for tilgang. Som tiltaket over, vil dette heller ikke dreie seg om et inngripende personvernmessig tiltak.

4.5.3 Adgangskort

Bruk av adgangskort sikrer at en begrenset krets av personer får tilgang til et område. Men bruk av adgangskort gjør at det kan registreres opplysninger om hvem som ferdes i et område, og også hyppighet og varighet av oppholdet. I noen tilfeller kan man også bruke adgangskortet til å registrere tidspunktet den ansatte kom eller gikk til et område. Vi er da straks inne på Personopplysningslovens område, som gjelder for alle former for ”behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler”, jf. § 3 a. Adgangskort (eller nøkkelkort) vil være nettopp et slikt elektronisk hjelpemiddel. For at kontrolltiltaket da skal være lovlig kreves det enten lovhjemmel, samtykke fra arbeidstakeren eller at tiltaket er nødvendig ut fra visse angitt formål, jf. § 8. Ved siden av samtykke vil det være særlig alternativene i § 8 a og f som er særlig aktuelle i arbeidsforhold. For adgangskort vil nok alternativ f kunne komme til anvendelse:

> ”at den behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen”.

Det følger vider av personopplysningslovens § 11 at formålet med behandlingen må være angitt før behandlingen settes i verk. Formålet skal være saklig begrunnet i arbeidsgivers virksomhet. Behandlingen vil være lovstridig om formålet ikke er angitt eller om opplysningene brukes utenfor formålet.

I vårt tilfelle kan altså arbeidsgiver etablere et adgangskortsystem av sikkerhetsmessige grunner. Men arbeidsgiver kan ikke så starte å benytte adgangskortsystemet til å registrere om de ansatte kommer for sent til jobb eller ikke, hvis arbeidsgiver ikke først informere de ansatte om at adgangskortet vil bli tatt i bruk til slik kontroll. For å forhindre industrispionasje vil arbeidsgiver hovedsaklig være interessert i adgangskort som et sikkerhetstiltak, og vil ha mulighet til dette ut fra loven.

4.5.4 Fjernsynsovervåke området

Fjernsynsovervåking er et kontrolltiltak som er regulert av Personopplysningslovens regler. Jeg behandler dette tiltaket under punkt 4.5 om overvåking av de ansatte.

4.6 Overvåking av de ansatte

4.6.1 Fjernsynsovervåking.

Gjennom videoovervåking vil arbeidsgiver kunne overvåke bedriften slik at uvedkommende blir oppdaget, eller en ansatts illojalitet blir fanget opp. I kapittel 3 ble ulike grunnlag for arbeidsgivers kontrolladgang behandlet. Som vi så vil det være begrensninger i kontrolladgangen. Når det gjelder videoovervåking eller fjernsynsovervåking vil disse begrensningene nå følge av personopplysningsloven, spesielt kapittel VII.[51] Rettspraksis fra før personopplysningsloven trådte i kraft vil likevel være av interesse, da rettspraksis gir et bilde av den vurderingen som retten legger til grunn og jeg vil her først se på to sentrale Høyesterettsdommer.

Rt. 1991 s. 616 gjaldt spørsmål om avskjæring av videoopptak foretatt i hemmelighet av arbeidsgiver. Arbeidsgiveren hadde misstanke om at en ansatt ved hans gatekjøkken begikk underslag. Det var for en tid tilbake blitt montert et kamera med monitor i

[51] Se punkt 3.6

forståelse med de ansatte. Men uten å informer arbeidstakerene koblet arbeidsgiveren kameraet til en videoopptaker. Ut fra opptakene som så ble gjort, mente han å kunne bevise at en av de ansatte begikk underslag ved flere anledninger.
Høyesterett åpnet for at slikt opptak kan være i strid med aml. § 12 eller § 19, men fant det ikke lovtolkningsspørsmålene avgjørende. De la vekt på at hemmelig videoovervåking av de ansatte på arbeidsplassen er at alvorlig inngrep i arbeidsmiljøet, og viste til at vesentlige personvernhensyn talte for at beviset ikke skulle tillates benyttet. Retten uttalte:

> "Selv om det kan være diskutabelt om hemmelige videoopptak på arbeidsplassen rammes av positive lovbestemmeleser, er det etter min oppfatning klart at fremgangsmåten medfører et slikt inngrep i den personlige integritet at den ut fra alminnelige personvernhensyn i utgangspunktet bør anses uakseptabel."[52]

Høyesterett fant derfor at beviset ikke kunne bli tillatt ført for retten da hensynet til sakens opplysning ikke ble ansett tilstrekkelig tungtveiende.

En lignende avgjørelse finner vi i Rt. 2001 s. 668. Også i denne saken ble det hemmelige videoopptaket nektet ført, selv om denne saken til forskjell fra saken over gjaldt en avskjedssak og ikke en straffesak. Arbeidsgiver hadde i dette tilfellet montert et videokamera uten å informere de ansatte for å finne ut om noen stjal fra tippekassen. Det var for øvrig annen videoovervåking av butikken som det var satt opp informasjon om, men kameraet som var montert til å overvåke tippekassen var skjult og bare satt opp for å overvåke de ansatte. Kjæremålsutvalget uttalte:

> "Ei slik særskilt, hemmeleg og føremålsretta overvaking representerer eit vidtgåande integritetsinngrep i høve til dei tilsette. Sjølv om også ei alminneleg videoovervking av eit butikklokale vil kunne fange inn tilsette, er karakteren av denne ei anna enn av ei slik målretta overvaking av dei tilsette. Klare personvernomsyn talar etter utvalet sitt syn for at eit slikt opptak i utgangspunktet ikkje er skaffa fram på lovleg måte"[53]

Kjæremålsutvalget fant også her at slik overvåking er særlig krenkende for de ansatte, og at tungtveiende personvernhensyn gjorde at beviset ikke kunne bli ført for retten

Vi ser av disse to dommene at Høyesterett legger vekt på kriterier som saklighet, forholdsmessighet og saksbehandlingen forut for tiltaket. I popplyl. § 37 jf. § 8 gir grunnvilkårene for all fjernsynsovervåking. Etter ordlyden i loven er det tre vilkår som

[52] RT 1991 s. 616

[53] RT 2001 s. 668

må være oppfylt for at fjernsynsovervåking skal være tillatt. Disse vilkårene er at tiltaket er nødvendig for å ivareta interessen til bedriften, denne interessen må være saklig, og ulempene for den som overvåkes må ikke være større enn fordelene med tiltaket. Som vi ser er disse grunnvilkårene svært like det som kommer frem av Høyesterettsdommene over.

En kjennelse fra Gulating lagmannsrett[54] i en arbeidsrettssak ble avsagt 15.10 01. Saksforholdet var relativt likt som i de foregående sakene. Arbeidsgiver foretok videoopptak med skjult kamera for å avdekke straffbare forhold fra de ansatte. I dette tilfellet var det misstanke om at den ansatte det gjaldt, drev manipulering av de faste overvåkningskameraene i lokalet. Arbeidsgiver bestemte seg derfor for å montere et kamera for å avdekke dette forholdet og kunne da selvsagt ikke informere de ansatte. Lagmannsretten kommer i dette tilfellet frem til at de hemmelige videoopptakene skal kunne fremlegges som bevis, selv om tidligere rettspraksis går i motsatt retning.
Det uttales:

> ”Når det gjelder videoopptaket i Space world-avdelingen er lagmannsretten enig i at dette opptaket rent faktisk har mange likhetstrekk med opptak omhandlet i Rt. 1991 s.616, men finner at resultatet likevel bør bli et annet i dette tilfellet.”

Lagmannsretten ser på den tidligere rettspraksis og viser til at man vanligvis avviser slike opptak. Det uttales at det ikke kan være legitimt å drive skjult videoovervåking av de ansatte selv om det kan sies å være en statistisk fare for ulovligheter. Lagmannsretten sier at det må i tilfelle foreligge svært spesielle omstendigheter for at slike videoopptak skal kunne tillates ført som bevis i en arbeidsrettssak. Man vektlegger i den forbindelse avdekking av kriminalitet og avkrefting av mistanke mot uskyldige som legitime formål ut fra et samfunnsmessig perspektiv. Retten uttaler:

> ”Etter lagmannsrettens oppfatning tilsier dette at domstolene i visse tilfeller må foreta en proporsjonalitetsvurdering av inngrepets karakter og alvorlighet, herunder videoovervåkingens innretning og avgrensning i tid og rom.”

Det blir lagt vekt på at den ansatte i denne saken utviste en særlig utspekulert og illojal handlemåte ved at det ble foretatt manipulering av de øvrige overvåkningskameraene. Det konkluderes tilslutt med:

---

[54] RG 2002 s. 162

> ”Lagmannsretten er således kommet til at videoopptakene i dette tilfellet representerer en inngrep i personvernet som må tåles i et rettssamfunn, og som derfor heller ikke bør avskjæres som bevis i den foreliggende sak.”

Lagmannsretten foretar her en proporsjonalitetsvurdering hvor samfunnmessige betraktninger som avdekking av kriminalitet måles opp mot personvernhensyn. Dette er i samsvar med de kriteriene som skal legges til grunn etter popplyl. § 37, jf. § 8. Avgjørelsen er interessant da den viser at arbeidsgiver i spesielt skjerpede situasjoner kan bli berettiget til å ta i bruk hemmelig overvåking overfor de ansatte.

En arbeidsgiver vil gode grunner for å bruke videoovervåking som et kontrolltiltak mot industrispionasje. Alle de nevnte kriteriene må da vurderes. Er et slikt tiltak nødvendig for å beskytte interessene (altså bedriftshemmelighetene) til bedriften?
Er det saklig å ville beskytte bedriftshemmelighetene? Hva blir ulempene for de ansatte i forhold til hva som oppnås ved å bruke videoovervåking?
De to første spørsmålene er lette å besvare med et ja. En bedriftshemmelighet kan ofte utgjøre hele grunnlaget for en bedrifts eksistens, og det klart at det vil være en saklig interesse for en bedrift å verne om disse. Det er hovedsaklig ulempene for de ansatte opp mot fordelene ved tiltaket som må vurderes. I mitt tenkte tilfelle med en bedrift som ønsker å forsvare bedriftshemmelighetene sine for å ikke miste sin konkurranse evne, vil gode grunner tale for at videoovervåking blir godtatt som kontrolltiltak. Bedriften installerer for eksempel kameraer som overvåker områdene rundt bedriften. Bedriften må da varsle om at slik overvåking foregår, jf. Popplyl. § 40. Dette må gjøres på en tydelig måte, og skilter som opplyser om dette og i tillegg hvem som er ansvarlig for overvåkingen vil være en grei måte å gjøre dette på.
Inne i bedriften vil man mest sannsynlig være ute etter å overvåke områdene hvor hemmelighetene oppbevares eller utarbeides. Det er da viktig at informasjonsplikten til de ansatte i bedriften overholdes, slik at tiltaket er blitt drøftet med de ansatte og de har blitt tilstrekkelig informert.[55]
Om bedriften kan bruke hemmelig videoovervåking er et annet separat spørsmål. Jeg har her tatt utgangspunkt i en arbeidsgiver som ønsker å beskytte seg mot industrispionasje. Arbeidsgiver vil derfor i utgangspunktet ikke ha behov for å ta i bruk hemmelig overvåking, da formålet uansett er å overvåke hemmelighetene og dette

[55] Som behandlet i kapittel 3

gjøres greit ved å bruke overvåking som det opplyses om og som er i forståelse med de ansatte. Hemmelig overvåking er i utgangspunktet ikke tillatelig verken etter loven eller rettspraksis. Men, hemmelig overvåking blir mest aktuelt i de tilfellene hvor arbeidsgiver har en konkret mistanke om at noen begår en forbrytelse mot bedriften. Ut fra personopplysningslovens kriterier og den nevnte rettspraksis kan mye tyde på at man er mer tillatelig til å godta slik overvåking i visse tilfeller hvor det dreier seg om forbrytelser. Men utgangspunktet er likevel at det er politiets oppgave å ta seg av etterforskning av forbrytelser, og en bedrift vil ikke kunne stå fritt til å sette i gang diverse hemmelige tiltak for å avklare slike forhold.

4.7 Telefonbruk

Det vil her dreie seg om den ansattes bruk av fasttelefon og mobiltelefon på arbeidsplassen. Jeg vil i den følgende drøftelsen forutsette at arbeidsgiver ikke betaler for hjemme telefonen til den ansatte. Private samtaler sier det seg selv at arbeidsgiver ikke vil ha noen interesse av, og det er enkelt å forhindre at private samtaler forekommer i arbeidstiden ved å innføre forbud mot dette. Selvsagt må det eksistere en mulighet for den ansattes familie og venner å komme i kontakt med denne ved alvorlige tilfeller. Dette vil da for eksempel kunne gå gjennom et sentralbord, som så enten kaller opp den ansatte og setter gjennom telefonen, eller som videreformidler beskjeden på annen måte. Arbeidsgiver kan riktignok ikke forby de ansatte å eie en mobiltelefon, men slik som mobilteknologien har utviklet seg i dag må det være adgang for arbeidstaker å nekte de ansatte å bringe telefonen inn på arbeidsplassen. I dag har de fleste mobiltelefoner innbygget fotokamera, videoopptak og noen har også lydopptaksfunksjon. Videre er de fleste telefonene utstyrt med WAP[56], som innebærer at mobiltelefonen kan knyttes opp mot Internett. De moderne mobiltelefonene kan fort bli et spionverktøy hvor den ansatte kan ta bilder av hemmelig materiale og så sende det via WAP systemet. Det sier seg da selv at en arbeidsgiver som ønsker å beskytte sine bedriftshemmeligheter bør være skeptisk til bruk, ja til og med til oppbevaring, av mobiltelefon på arbeidsplassen.

[56] Wireless Access Point

I svært mange arbeidssituasjoner er man likevel nærmest avhengig av at de ansatte er lett tilgjengelige på telefon, og mobiltelefoner er derfor svært vanlige på de fleste arbeidsplasser. Arbeidsgiver kan ved å dele ut mobiltelefoner til de ansatte som ikke har funksjoner som for eksempel kamera og lydopptak, unngå at telefonene utgjør en fare for sikkerheten. Arbeidsgiver kan da bestemme at telefonen kun skal brukes i jobbsammenheng.

4.7.1 Avlytting av fasttelefonen

Kan en arbeidsgiveren avlytte telefonsamtalene som går ut eller kommer inn til arbeidsplassen? I utgangspunktet bør ikke slik avlytting forekomme.
I en avgjørelse fra Menneskerettighetsdomstolen 25. juni 1997 ble det vist til EMK artikkel 8 om retten til respekt for privatliv i en sak hvor det var foretatt avlytting av telefonsamtaler på et kontor. En arbeidstaker må kunne forvente å ha rett til private samtaler når ikke annen beskjed er gitt.[57]
Dette kan knyttes opp til prinsippet om varsel om overvåking i popplyl. § 40. Ut fra dette kan det altså være at det stiller seg annerledes hvis den ansatte har fått informasjon på forhånd om at slik avlytting vil bli foretatt, og hvis den ansatte har samtykket i slik avlytting. Samtykke må i så fall være klart og entydig, og den ansatte må være fullt inneforstått med hva tiltaket innebærer.[58]
En avisartikkel i Dagsavisen av 14. september 2003, omhandler arbeidsgivers adgang til kontroll av effektiviteten. Datatilsynet stiller seg her skeptisk til avlytting av telefonsamtaler selv om arbeidstaker har samtykket i slik avlytting. De mener at det er usikkert hvor frivillig et slikt samtykke er i dagens pressede arbeidsmarked. Det er godt mulig at Datatilsynet vil legge den samme tolkningen til grunn ved spørsmål om avlytting av telefonsamtaler for å kontrollere at ikke industrispionasje forekommer, selv om den ansatte er innforstått med at slik kontroll vil bli foretatt. Men det er viktig å merke seg at i den nevnte avisartikkelen gjaldt det kontroll av effektiviteten til en arbeidstaker, mens det som tiltak mot industrispionasje vil dreie seg om kontroll mot illojale handlinger. Dette formålet for kontroll må kunne sies å være mer akseptabelt enn et effektivitetshensyn. Likevel vil avlytting være et svært inngripende tiltak i den

[57] Se Dege, 2003

[58] Se punkt 3.2.2

personlige integriteten til arbeidstaker, og det vil mest sannsynlig måtte stilles strenge krav til forhåndsinformasjon av de ansatte og et eventuelt samtykke.

4.7.2 Kontroll av telefonbruk

Mange telefonsystemer kan i dag registrere varighet, tidspunkt for samtalen og hvem som ringte eller ble oppringte. Hvis disse opplysningene kan knyttes til en enkelt arbeidstaker vil dette være personopplysninger som faller inn under personopplysningslovens virkeområde.
Bedriftens interesse for å kontrollere slik telefonbruk må da vurderes opp mot hensynet til de ansatte etter de samme kriteriene som ved andre kontrolltiltak, jf. punkt 4.6 om overvåking. Også her vil det spille inn om arbeidsgiver på forhånd har informert om at slik kontroll vil bli utført, og om den ansatte eventuelt har samtykket i et slikt tiltak.

Ut fra den tenkte situasjonen i denne oppgaven, vil nok mye tale for at arbeidsgiver kan foreta slik kontroll hvis kriteriene ellers er oppfylt.

4.7.3 Kontroll av mobiltelefon

Mobiltelefoner lar seg i utgangspunktet ikke avlytte på samme måte som en fast telefon. Det finnes systemer i dag som kan klare å avlytte en mobiltelefon, men dette er såpass spesielt at jeg i denne oppgaven legger til grunn at arbeidsgiver ikke kan avlytte de ansattes mobiltelefon.

Som sagt innledningsvis, legger jeg her til grunn at det dreier seg om kontroll av en mobil som er fullt ut betalt av arbeidsgiver, og som det på forhånd er klarlagt og avtalt at kun skal brukes i jobbsammenheng av sikkerhetsmessige årsaker. Det samme som er sagt i punket over vil også gjelde her, og mest sannsynlig vil arbeidsgiver kunne foreta kontroll av oppringte og mottatte telefonsamtaler.

Hvor en mobiltelefon eller annen telefon også kan brukes til private formål vil arbeidsgiver ikke ha den samme adgangen til kontroll, da det vil være et brudd på personopplysningsloven.[59]

[59] For mer om dette se Dege, 2003

4.8 Kontroll av aktivitetslogg

En aktivitetslogg er en totaloversikt av all elektronisk trafikk i bedriftens datanettverk. Vi må her skille mellom bedriftens behov for å kontrollere at systemet er i orden slik at ikke viktig arbeide skal gå tapt, og behovet for å kontrollere ansattes prestasjon i løpet av en arbeidsdag. Det siste er også et interessant spørsmål, men har ingenting med problemstillingen i denne oppgaven og gjøre, og jeg henviser i stedet til Datatilsynet og personopplysningsloven.

En bedrift som skal forsvare seg mot industrispionasje vil ha en viss interesse av å kunne kontrollere slike logger, forutsatt at bedriften faktisk har tillatt bruk av Internett på arbeidsplassen. Da et slikt tiltak likevel ikke direkte kan sies å forhindre industrispionasje, men mer å forhindre at de ansatte ikke missbruker arbeidstiden sin og eventuelt kontrollere at de ansatte ikke er innen på uønskede internettområder, vil jeg ikke behandle denne form for kontroll inngående.

Innledningsvis kan nevnes at arbeidsgiver er ikke pålagt å ha Internett på arbeidsplassen. Styringsretten tilsier at arbeidsgiver kan både la vær å ha Internett, eller forby de ansatte å bruke det eller i hvert fall sperre for visse internettområder.
Hvis man likevel velger å la de ansatte bruke Internett, blir spørsmålet om arbeidsgiver kan kontrollere bruken av det. Når den ansatte bruker Internett, sender e-post eller jobber i systemet for øvrig, lagres dette i aktivitetsloggen. Denne loggen vil inneholde opplysninger om hvem som er bruker, hvilke sider som er besøkt, hvor lenge man var inne på disse sidene, eller tiden det tok å skrive en e-post. Man har slike logger for å kunne administrere og vedlikeholde systemet. Hvis det oppstår en feil vil man ved hjelp av aktivitetsloggen kunne finne ut hvor feilen oppstod. Slik automatisk loggføring er elektronisk behandling av personopplysninger og omfattes derfor av personopplysningsloven.
En arbeidsgiver som søker å unngå industrispionasje, vil det være en hjelp å bruke kontroll av aktivitetsloggen til å for eksempel studere om det foregår mye aktivitet i filene som inneholder bedriftshemmelighetene. Ved hjelp av loggen vil man kunne se om det for eksempel foregår nedlasting av filer som inneholder bedriftshemmeligheter.

I Rt. 2001 s. 1589 ble en IT-konsulent (A) avskjediget fordi A hadde brukt arbeidsgivers internettlinjer til private formål og blant annet lastet ned et betydelig antall

musikkfiler fra nettet. Ved å laste ned disse filene, brukte han ikke bare arbeidstiden til private gjøremål, men han svekket også systemkapasiteten slik at andre brukere ikke kom inn og fikk gjort jobben sin. På grunn av bedriftens problemer med kapasiteten på Internettlinjen sin, besluttet IT-sjefen å ta utskrift av loggen over den interne internettbruken. Dette ble gjort på en tilfeldig valgt dato. Det viste seg da at A's to Pc-er stod for ca 50 % av nedlastningen og flere loggutskrifter viste det samme mønstret. IT-sjefen og en annen kollega låste seg derfor inn på kontoret til A etter arbeidstid og tok en katalogutskrift fra en av PC-ene til A hvor det viste seg at det ble lastet ned store mengder musikkfiler. Det ble fremholdt for Høyesterett at bedriften med disse handlingene hadde overtrådt grensen både for det lovfestede og det ulovfestede personvern. Høyesterett avviser dette og viser til at utskriften som ble tatt av aktivitetsloggen på den tilfeldig valgte datoen var i samsvar med datidens personregisterlovens hovedforskrift § 2-20 . Det fremgikk av forskriften at et register over aktiviteter internt i et edb-system eller datanett, bare kunne brukes til administrasjon av systemet, og til å avdekke eller oppklare brudd på sikkerheten i edb-systemet.[60] Høyesterett sier at undersøkelsen av aktivitetsloggen er å betrakte som "administrasjon av systemet" slik forskriften sier er tillatt, og den er heller ikke til hinder for at bedriften gikk videre med den informasjonen de fikk ut av undersøkelsen om A. Når det gjaldt rettmessigheten av å låse seg inn på kontoret til A fant retten at dette var i samsvar med hva som var vanlig akseptert på arbeidsplassen.

Behandling av logger går i dag under personopplysningsforskriften § 7-11, og unntatt fra meldeplikt etter popplyl. § 31 første ledd. Men unntaket gjelder kun behandling som skal administrere systemet eller oppklare feil i sikkerheten.

4.9 Kontroll av personlig post

Åpning av en annen persons post er straffebelagt etter strl. § 145 første ledd, forutsatt at brevbruddet er uberettiget. En arbeidsgiver vil ikke kunne åpne og kontrollere brev som er sendt til den ansatte som privatperson. Noe annet er om brevet er adressert til bedriften men ved en spesiell ansatt, men ellers klart fremstår som et forretningsbrev. Da vil en annen enn den brevet er adressert til kunne åpne brevet.

[60] Bestemmelsen er i det vesentlige videreført i den nåværende personopplysningsforskriften, § 7-11.

4.10 E-post[61] og private bruker områder

En spion kan bruke e-post til å sende ut sensitive opplysninger fra bedriften eller det kan være generell kommunikasjon med en konkurrent som vil ha hemmeligheter. Arbeidsgiver kan på dette grunnlag ha en interesse i å ha kontroll med de ansattes e-post.

I en avgjørelse fra RG 1993 s. 77 er vi inne på noe av den samme problematikken. Her hadde administrerende direktør gått inn på arbeidstakerens private brukerområde i bedriftens databaserte postsystem uten at det var klarlagt på forhånd at arbeidsgiver skulle ha adgang til å foreta en slik kontroll. I brukerveiledningen til systemet var det oppgitt at dette området var privat, og at ingen andre ville ha tilgang med mindre de hadde lese- eller skrivetilgang til den aktuelle disk. Retten fant det ikke tvilsomt at bedriften måtte ha adgang til bedriftsinformasjon som fantes på "åpne brukerområder", og la videre til grunn at bedriften i utgangspunktet også måtte ha adgang til å gå inn på den enkeltes private brukerområder hvis det var fastsatt regler eller instruks som ga ledelsen en slik adgang og de ansatte var gjort kjent med disse bestemmelsene. Handlingen fra den administrerende direktøren var derfor å betrakte som et inngrep i den personlige integritet ut fra alminnelige personvernregler.

Det går frem av dommen at arbeidsgiver kan ha rett til å gå inn på de private brukerområdene, men dette må da være opplyst om og avtalt på forhånd.
Som utgangspunkt må arbeidsgiver ha samtykke fra arbeidstaker om å lese privat e-post.
Rettslig kan e-post likestilles med vanlig post i brevs form i konvolutt. Hvis arbeidsgiver uberettiget leser slik privat e-post kan strl. § 145 annet ledd være overtrådt. Av denne bestemmelsen fremgår det at det er straffbart å "bryte en beskyttelse eller på lignende måte uberettiget" skaffe seg adgang til "data eller programutrustning som er lagret eller som overføres ved elektroniske eller andre tekniske midler".
Virksomhetsrelatert e-post må arbeidsgiver kunne lese, da denne vil ha en berettiget interesse i innholdet i denne typen e-post. Dette kan særlig være aktuelt hvis den ansatte blir syk og borte over en lengre periode og det er behov for at noen andre håndterer

[61] Elektronisk-post

jobbrelevant e-post som kommer inn. Det må likevel forutsettes at arbeidsgiver har informert arbeidstaker om at dette kan forekomme på forhånd.

Det enkleste for å forhindre industrispionasje vil være at arbeidsgiver forbyr de ansatte å bruke bedriftens datasystem til private formål. Det må da kunne antas at arbeidsgiver vil ha rett til å slette eventuell privat e-post hvis de ansatte allikevel bruker systemet til dette, men arbeidsgiver vil fortsatt ikke ha noen rett til å lese privat e-post. På bakgrunn av dette må det gis arbeidsgiver et visst spillerom for å sjekke hva som er privat e-post og hva som er virksomhetsrelatert.

4.11 Undersøkelser av den ansatte

For å unngå at noen ansatte klarer å ta med seg enten viktige papirer, tegninger, bilder, formler eller vareprøver, vil et aktuelt kontrolltiltak være undersøkelse av den ansatte og dennes private kjøretøy. Med slik undersøkelse forstår en både kroppsvisitasjon og ransaking. Kroppsvisitasjon vil innebære foruten undersøkelse av kroppens hulrom, undersøkelse av klær, vesker og andre gjenstander som bæres på kroppen. Ransaking innebærer undersøkelse av andre personlige ting som garderobeskap, privat kjøretøy og bagasje. Adgangen til slike undersøkelser er klarlagt i norsk rett[62], men det finnes noen eksempler fra rettspraksis på området.

4.11.1 Personkontroll, undersøkelse av vesker m.m.

I ARD 1951 s. 201 var det to bryggerier som hadde innført person kontroll ved inn- og utpassering fra bedriften. Alle som passerte skulle trykke på en knapp som lyste grønt eller rødt. Ved rødt lys ble man underlagt kontroll. Kontrollen var ikke begrunnet i konkret misstanke mot noen, og fungerte vilkårlig da det ikke var noen spesiell gruppe som ble valgt ut for kontroll. Kontrollen var nedfelt i tariffavtale mellom arbeidsgiverforeningene (NAF og BAF) og de ansattes forbund (NNN) hvor det bl.a. var bestemt:

[62] Se punkt 3.4

> ”Kontrollen skal omfatte samtlige som passerer ut av bedriftene (herunder også eksempel vis kunder som har hentet varer) og søkes gjennomført så effektivt som mulig”. [63]

Noen installatører som ikke var ansatt ved bryggeriene ville ikke la seg kontrollere etter å ha vært på oppdrag ved de aktuelle bedriftene. De var ikke omfattet av den nevnte tariffavtalen, men ble pålagt av sin arbeidsgiver å underkaste seg kontroll. Arbeidsretten la til grunn av arbeidsgiver hadde lov å pålegge installatørene å underkaste seg nødvendig kontroll og viste bl.a. til de tungtveiende formålene bak kontrollen og at installatørene ikke hadde noen grunn til å føle seg krenket ved kontrollen.

4.11.2 Undersøkelser av bil eller annet transportmiddel

ARD 1978 s. 110 gjaldt stikkprøvekontroll av de ansattes privat kjøretøyer.

Arbeidsretten viste til tidligere avgjørelser og uttalte:

> ”Gjennom ARD 1937 s. 114 flg., ARD 1951s. 201 flg., ARD 1958 s. 189 flg., ARD 1968 s. 44 flg. har Arbeidsretten fastslått at bedriftene i kraft av sin styringsrett har tariffrettslig adgang til å iverksette kontrolltiltak av forskjellig karakter overfor arbeidstakerne. Vilkåret for at det foreligger en slik adgang er imidlertid at det sakelig sett er behov for vedkommende kontrolltiltak og at tiltaket ikke praktiseres vilkårlig, i den mening at man uten reell begrunnelse setter enkelte arbeidstakergrupper i særstilling. I denne forbindelse er det dessuten å merke at kontrolltiltaket ikke på tariffrettslig holdbar måte kan innføres med mindre informasjons- og drøftelsesplikten i Hovedavtalens § 9 punkt 2 er blitt lojalt etterlevet.” [64]

Arbeidsretten konstaterte så at informasjons- og drøftelsesplikten etter Hovedavtalen var oppfylt og sier så:

> ”Etter det opplyste må det videre antas bedriftenes vurdering av behovet for enkeltvis stikkprøvekontroll av de ansattes kjøretøyer på ingen måte kan tilsidesettes som åpenbart grunnløs eller som motivert av utenforliggende hensyn. Endelig kan det ikke sees at den praktiserte kontroll etter sin karakter påfører arbeidstaker ulemper av en slik størrelsesorden at kontrollen av den grunn er tariffrettslig angripelig”[65]

---

[63] Se Artikkelsamling i arbeidsrett, 2001 (Jakhelln ”Om arbeidsgivers kontrolladgang”)

[64] ARD 1978 s. 110

[65] ARD 1978 s. 110

4.11.3 Oppsummering av adgang til personkontroll

De to nevnte dommene viser at arbeidsgiver har en relativt vid adgang til å foreta personkontroll basert på styringsretten. En vil likevel være nødt til å se på formålet med tiltaket og se om dette er nødvendig og ikke fremstår som uforholdsmessig.

Når det gjelder kroppsvisitasjon er dette et svært inngripende tiltak som vanligvis er forbeholdt politiet, og det foreligger strenge krav om lovhjemmel før noe slikt kan foretas. Styringsretten til arbeidsgiver vil altså ikke gi grunnlag for å foreta en kroppsvisitasjon. Det kan tenkes unntak hvor svært tungtveiende sikkerhets- og risikohensyn gjør seg gjeldende sammen med sterke almene hensyn.[66] Faren for industrispionasje vil mest sannsynlig ikke være tungtveiende nok når det dreier seg om et så personvernmessig inngripende tiltak. Det kan likevel tenkes at samtykke fra den ansatte kan gi grunnlag for å foreta slik kontroll, men det må da stilles strenge krav til samtykkes form og informasjon gitt i forkant om tiltaket.

4.12 Undersøkelse av den ansatte utenfor arbeidstiden

Arbeidsgivers behov for å være sikker på at viktig informasjon ikke har kommet seg ut fra bedriften slutter kanskje ikke ved ransakning og veskeundersøkelser. Man tror kanskje at en ansatt har klart å få med noe ut og ønsker derfor å undersøke huset eller til og med hytten eller seilbåten til den ansatte.

4.12.1 Undersøkelse av hus, hytte eller annen fritidseiendom

Her er vi straks over på et langt mer komplisert område. Det kan ikke sies å foreligge noe rettslig grunnlag verken ut fra skrevne lover eller ulovfestet rett som gir arbeidsgiver en slik rett. Det vil her være snakk om store inngrep i privatlivet til den enkelte, og etter dagens lovverk er det kun politiet som kan ha en slik rett.
Igjen må vi se hen til arbeidsgivers formål og hensikt med en slik undersøkelse. Arbeidsgiver vil forsikre seg om at intet materiale er tatt med ut fra bedriften slik at det er en trussel for hans konkurransedyktighet.

---

[66] Se Underutvalgets rapport, 2002

Hvor arbeidsgiver har en konkret mistanke om misligheter av en viss betydning, vil det kunne tale for at arbeidsgivers adgang til kontroll går noe lenger. Man skal ikke strekke denne muligheten for langt, da det fortsatt er politiet som har ansvar for oppklaring av forbrytelser. I et tilfelle hvor arbeidsgiver har en konkret mistanke om at en ansatt har tatt med seg bedriftshemmeligheter hjem, kan det tenkes at det er en mulighet for arbeidsgiver til å kontrollere hjemmet til den ansatte for å avkrefte mistanken. Både den ansatte og arbeidsgiver vil ha en viss interesse av å oppklare forholdet. Mest sannsynlig vil den ansatte kunne samtykke i at arbeidsgiver skal kunne komme til dennes hjem for å foreta en slik undersøkelse. Noe annet er hvis den ansatte siden trekker tilbake et slikt samtykke og så motsetter seg slik undersøkelse. I en dom fra Oslo byrett fra 11. februar 1983 gjaldt oppsigelse av en ansatt som var mistenkt for å ha stjålet fra bedriftens delelager. Avskjeden ble underkjent, men retten fant at vilkårene for saklig oppsigelse forelå. Det ble lagt en viss vekt på at arbeidstakeren hadde unnlatt å medvirke til gjennomføringen av et planlagt kontrollbesøk i hennes hjem for å avkrefte mistanken om tyveriet. Denne dommen tyder på at slike undersøkelser kan forekomme, og at arbeidstakers oppførsel rundt en slik kontroll kan bli tillagt vekt ved en eventuell oppsigelse.

4.13 Tiltak mot arbeidstakers utnyttelse av bedriftshemmelighet etter arbeidsforholdet tar slutt

Industrispionasje trenger ikke bare forekommer mens arbeidsforholdet eksisterer. Mange mennesker jobber flere steder i løpet av sin yrkeskarriere. Hvis en ansatt slutter i bedriften og startet opp for seg selv eller får arbeid hos en annen bedrift, vil tidligere arbeidsgiver ha god grunn til å frykte at personen som sluttet på en eller annen måte vil utnytte de bedriftshemmeligheter han måtte ha fått innsyn i. Jeg vil i det følgende se på hva arbeidstaker kan gjøre for å forhindre at slik utnyttelse forekommer.

Å søke å forhindre at en tidligere ansatt utnytter kunnskaper denne har tilegnet seg gjennom ansettelsesforholdet er beslektet med problematikken rundt konkurranse med tidligere arbeidsgiver. I mitt tilfelle dreier det seg likevel ikke om å forhindre at den ansatte starter opp en virksomhet som blir konkurranse med tidligere arbeidsgiver, men man er ute etter å forhindre missbruk av bedriftshemmeligheter.

4.13.1 Lovbestemmelser

Vi har bestemmelsen i strl. § 294 nr.2 som rammer den som ”uberettiget enten selv gjør Brug af en Forretnings- eller Driftshemmelighet” som tilhører en bedrift denne jobber for eller har jobbet for. Strl. § 294 nr.2 fanger også opp det å gi videre bedriftshemmeligheter til andre. Denne bestemmelsen begrenser seg ikke til næringsvirksomhet, men rammer en hver situasjon som gjelder utnyttelse av bedriftshemmeligheter.
Strl. § 294 nr.2 setter en grense ved to år. Tidsfristen er der for å hindre at en ansatt skal føle seg fristet til å slutte hos sin arbeidsgiver for å så direkte til en konkurrent eller starte sin egen virksomhet og derigjennom benytte hemmeligheten.[67]
Vi har altså lovbestemmelser som gjør det ulovlig for en tidligere ansatt, (eller noen andre som denne videreformidler informasjon til), å utnytte bedriftshemmeligheter. Straffetrusselen vil være bøter eller fengsel mellom 3 til 6 måneder, alt etter hvilken bestemmelse forholdet går under.

Mfl. § 7 første ledd setter forbud mot at næringsdrivende utnytter en bedriftshemmelighet mottatt ved brudd på taushetsplikt eller annen rettstridig handling. Mfl. § 17 gir bestemmelser om straff ved overtredelsen av § 7. I § 17 første ledd fremgår det at overtredelse av § 7 straffes med bøter eller fengsel i inntil 6 måneder eller begge deler ”dersom ikke strengere straffebestemmelse kommer til anvendelse”. Verken strl. § 294 eller § 405a gir strengere straff enn straffebestemmelsen i mfl. § 17.
§ 17 femte ledd fastsetter at det ikke gis straff for overtredelse av § 7 hvis det er gått mer enn to år siden tjeneste- eller tillitservervsforholdet er opphørt. Dette er helt i samsvar med § 294.

4.13.2 Lojalitetsplikten og taushetserklæringer

Som behandlet over foreligger det en lojalitetsplikt i et arbeidsforhold. Den alminnelige lojalitetsplikten vil i seg selv være til hinder for at en arbeidstaker kan utnytte bedriftshemmeligheter som denne har fått kunnskap om gjennom arbeidsforholdet.
I tillegg vil det ofte være taushetserklæringer som binder den ansatte ytterligere. [68]

---

[67] Se for øvrig Inst. fra konkurranselovkomiteen, 1966

[68] Se punkt 4.4

Gjennom disse taushetserklæringene vil arbeidsgiver kunne spesifisere hvilke forhold det ikke er tilgang til å snakke om. Brudd på en slik erklæring vil medføre ansvar etter de nevnte lovbestemmelser.

4.13.3 Konkurranseklausul

Ved forholdet konkurranse med tidligere arbeidsgiver er det ofte vanlig med konkurranse klausuler. Ut fra rettspraksis er det vanlige at disse ikke avtales å vare mer enn to år.[69] I vurderingen av om slike klausuler er rettmessige, vil man ofte seg på om arbeidsgiver har betalt et vederlag for perioden den ansatte ikke skal drive med konkurrerende virksomhet. Strl. § 294 nr.2 gir her arbeidsgiver en rett til at dennes hemmeligheter ikke benyttes i løpet av en to års periode. Men bestemmelsen sier ingenting om at den ansatte ikke kan ta seg jobb hos en konkurrent eller drive konkurrerende virksomhet. I praksis vil det være vanskelig å bevise at en ansatt har utnyttet en bedriftshemmelighet. Det kan derfor være lurt at en arbeidsgiver som ønsker og sikre seg mot at en tidligere ansatt blir fristet til å enten selv utnytte en bedriftshemmelighet eller gå til en konkurrent med disse, avtaler en konkurranseklausul. Jeg vil ikke her gå inn på problemstillingene rundt slike klausuler og gyldigheten av disse.[70]

5 Tiltak mot uaktsom industrispionasje

Som vist i punkt 2.7.2 er uaktsom industrispionasje et fenomen som svært lett kan forekomme. Jeg vil i det følgende forsøke å komme med forslag til noen tiltak som kan være med på å redusere problemet. Her som ellers må grunnlaget for arbeidsgivers adgang til å iverksette kontroll tiltak være arbeidsgivers styringsrett.[71]

5.1.1 Taushetsplikt og taushetserklæringer

Dette er nøye drøftet under kapittel 4 om kontrolltiltak mot den aktsomme industrispionasje i punkt 4.3. De samme hensyn og vurderinger vil gjelde her.

---

[69] se RG 1996 s. 1241 (og Jakhelln "Fjernarbeid" Complex 5/96)

[70] For mer om konkurranse med tidligere arbeidsgiver se artikkel av Alex Borch og Jan Fougner, 2000 i Artikkelsamling i arbeidsrett, 2001

5.1.2 Personlige forbud

Av og til føles det ikke tilstrekkelig for arbeidsgiver med taushetsplikt og erklæringer. I noen tilfeller vil det også være et behov fra arbeidsgivers side om å forsikre seg om at den ansatte er fullstendig klar over både hva denne ikke skal snakke om, og konsekvensene av brudd på dette. Arbeidsgiveren tar da kanskje et møte med den eller de ansatte det måtte gjelde, og gir et personlig forbud mot visse forhold innen bedriften. De sammen forhold ved et slikt forbud vil gjelde her som i drøftelsen i punkt 4.3 over, og det må foretas en vurdering av hva det er bedriften ønsker å pålegge et personlig forbud mot opp mot den ansattes mulighet til å si fra om forholdet.

5.1.3 Generell informasjon til de ansatte

Tiltakene over er vel og bra, men hva kan virkelig gjøres for å få de ansatte til å forstå at de er nødt til å utvise den aller største forsiktighet med hva de sier? Kanskje er noe av det viktigste i en bedrift å ha et godt og nært arbeidsmiljø hvor de ansatte føler seg trygge på sin arbeidsplass og trives med sitt arbeide. Bedriften bør derfor sørge for god kontakt med de ansatte og jevnlig kommer med informasjon både om konkurranse forhold utad og forholdene innad i bedriften. Videre kan man informere de ansatte om faren ved å utlevere informasjon og konsekvensene dette kan få for bedriften. I noen tilfeller kan man også vurdere og ha egne kurs som brifer de ansatte om situasjoner som nevnt i mine eksempler ovenfor, og hvordan de da bør forholde seg. På denne måten skaper man en samlet bedrift, og forhåpentligvis forhindre noen tilfeller av uaktsomhet.

6 Avslutning

Mens Sovjetunionen fortsatt bestod, og den kalde krigen var en del av datidens virkelighet, var det en særlig redsel for spioner fra øst som regjerte. I Teknisk ukeblad fra 1987 er det en artikkel med overskriften ”Slik unngår du spionene!”[72]. Denne artikkelen tar for seg faren fra øst, og kommer tilslutt med noen råd om hvordan man kan unngå spionene. Man rådes her til å være forsiktig med sosialt samvær med personer fra øst-blokk landene, og til å ikke være intime med innfødte hvis man er på

[71] Se for øvrig punkt 3.2.1 hvor styringsretten omtales nærmere.

[72] Bekkevold, 1987

reise i disse landene, da dette kunne medføre at man havnet i en situasjon hvor man enten ble vervet til å bli spion eller ble truet til det. Dette er råd som ikke akkurat lar seg nedfelle i lov eller fastsette i et internt forskrift i bedriften. Det dreier seg til syvende og sist om sunn fornuft og sosiale antenner, noe det er vanskelig å kontrollere at den ansatte har, slik det går frem i denne oppgaven rundt uaktsom industrispionasje.
I dagens samfunn, er fiende kanskje mer skjult enn noen gang. Det er ingen som kan pekes ut som en særdeles farlig fiende lenger, man er på vakt mot alt og alle. Åpenhet om både private og profesjonelle forhold preger samfunnet vårt, og vi kommuniserer mer enn noen gang tidligere med e-post, mobiler og tekstmeldinger. Informasjon har aldri vært mer tilgjengelig enn nå. Nettopp derfor er kanskje behovet for å beskytte seg både mot den aktsomme og den uaktsomme industrispionasjen sterkere enn noen sinne også. I New York i USA henger følgende skilt i korridorene og heisene i sykehusene: ”Don’t talk about patients, you don’t know who’s listening”.
I den travle verden vi lever i er det lett å glemme å være like påpasselig med hva man sier, man tenker ikke alltid over konsekvensene det kan få. Så da er det kanskje greit å ha arbeidsgivers konstante påminnelse rundt seg om å utvise aktsomhet?

Vi mangler fortsatt et samlet lovverk i Norge om bedriftshemmeligheter, men mest av alt mangler vi en definisjon av selve begrepet. Ragnar Knoph påpekte i 1934 viktigheten av å ha en slik definisjon, blant annet for å sette nøyaktige og klare grenser for hva som må sies å være et brudd på reglene. Man kan jo stille seg undrende til hvorfor man i 1960 og 1970 årene under utarbeidelsen av markedsføringsloven lar vær å gi en lovdefinisjon av begrepet bedriftshemmeligheter, når man ellers har valgt å vektlegge det Knoph sa i 1934. Sverige fikk sin lov om beskyttelse av bedriftshemmeligheter i 1990 med definisjon av bedriftshemmeligheter. Det er kanskje på tide at Norge følger etter? En ting er sikkert, slik konkurransen i næringslivet utvikler seg i dag, vil det ikke bli mindre kamp om bedriftshemmelighetene i fremtiden.

7 Litteraturliste

Bøker med opptil 3 forfattere

Bokmålsordboka, Definisjons- og rettskrivningsordbok. 2.utg. Oslo, 1986

Dege, Tormod. *Arbeidsrett, Rettigheter og plikter i arbeidsforhold.* Oslo, 2003

Fahlbeck, Reinhold. *Företagshemligheter, konkurrensklausuler och yttrandefrihet.* Göteborg, 1992

Fanebust, Arne. *Innføring i arbeidsrett, Den individuelle delen.* Oslo, 1997

Fanebust, Arne *"Oppsigelse i arbeidsforhold".* 3. utg. Oslo, 1995.

Heradstveit, Per Øyvind. *Spionasje og infiltrasjon i industrien.* Oslo, 1976

Iseskog, Tommy. *Skydd för företagshemligheter.* Stockholm, 1990

Jakhelln, Henning. *Oversikt over arbeidsretten.* 2.utg. Oslo, 1996

Knoph, Ragnar. *Bedriftshemmeligheters rettsbeskyttelse.* Oslo, 1934

Poulsen, Sune Troels. *Loyalitetspligt og erhvervsforbud.* Danmark, 1991

Wiik Johansen, Michal. *Personopplysningsloven, Kommentarutgave.* Michael Wiik Johansen, Knut-Brede Kaspersen, Åste Marie Bergseng Skullerud. Oslo, 2001

Redigerte verk

Artikkelsamling i arbeidsrett. Redigert av Henning Jakhelln. Oslo, 2001

Folkerettslige tekster. Redigert av Erik Møse. 4.utg. Oslo, 1995

Forhandlinger på Det sekstende Nordiske Juristmøte. Utgitt av Det Norske Styre. Oslo 1935

Enkelte bind i flerbindsverk eller serier

Jakhelln, Henning. *Arbeidsrettslige og rettslige studier.* Bind 2. Oslo, 2000.

Storeng, Beck og Due Lund. *Arbeidslivets spilleregler.* Bind 1, 2 og 3, Oslo, 2003

Artikler i tidsskrifter, årbøker, samleverk

Bang, Heidi Katrine. *Sjefen må spørre om lov til å sjekke ansatte.* I: Dagsavisen 2003, s.7

Bekkevold, Stein. *"Slik unngår du spionene!".* I: Teknisk ukeblad, Årg. 134,nr. 42, 1987 []

Jakhelln, Henning. *Ytringsfrihet om forsvarsforhold – "Ikkevold"-saken ex post.* I: JV 1990, hefte 2, s.73 – 94

Jakhelln, Henning. *Ytringsfrihet om forsvarsforhold – illusjon eller realitet?* I: JV 1987, hefte 6-7, s. 231 flg.

Elektroniske dokumenter

Underutvalgets rapport. *Kontroll og overvåking i arbeidslivet.* Avlevert til Arbeidslivslovutvalget 20.juni 2002. Hentet fra Odin nettsider. Tilgang: http://odin.dep.no/aad/arbeidslivslovutvalget/publikasjoner/p30000945/002081-220018/index-dok000-b-n-a.html [Sitert 18.10.03]

Forarbeider

Forarbeid til lovene 1972, bind II, *Forarbeider til lover nr. 23 – 72: Lov av 16. juni 1972 nr.47 om kontroll med markedsføring:*

- Innstilling fra konkurranselovkomiteen. Om ny konkurranselov. Otta, 1966.
- Ot.prp. nr. 57. (1971 – 72) Lov om markedsmisbruk.
- Inst. O. XIX – 1971 – 72 Kontroll med markedsføring

Odelstingsproposisjon nr. 56, 1992-93, Om lov om endring i lov 9.juni 1978 nr 48 om personregistre m.m.

Forkortelser

Innst. O. : Innstilling til Odelstinget

Ot. prp. : Odelstingsproposisjon

NOU : Norges offentlige utredninger

Rt : Norsk Retstidende

RG : Rettens Gang

Lovregistre

Norske lover

Kongeriget Norges Grundlov 17.mai 1814 (Grunnloven)

Almindelig borgerlig straffelov av 22.mai 1902 nr.10 (straffeloven)

Lov om kontroll med markedsføring og avtalevilkår 16.juni 1972 nr. 47 (markedsføringsloven)

Lov om arbeidervern og arbeidsmiljøloven m.v. av 4 februar 1977 nr.4 (arbeidsmiljøloven)

Lov om grunnskolen og den vidaregåande opplæringa av 17.juli 1998 nr.61, (opplæringslova)

Lov om behandling av personopplysninger av 14.april 2000 nr. 31 (personopplysningsloven)

Svenske lover

Lag om skydd för företagshemligheter av 1.juli 1990

Konvensjoner, resolusjoner, overenskomst, rekomenndasjoner etc.

European convention for the protection of human rights and fundamental freedoms, Roma 4. november 1950. (Den Europeiske Menneskerettskonvensjon)

International Covenant on Civil and Political Rights, 16.12. 1966. (Konvensjon om Sivile og politiske rettigheter)

ILO – Konvensjon nr. 111 1958

Tariffavtaler

Hovedavtalen mellom LO og NHO av 2002 – 2005

Tilleggsavtale V til Hovedavtalen LO- NHO (2002 – 2005)

Domsregister

Norsk Retstidende

Rt. 1937 s. 63 Hydro saken om industrispionasje

Rt. 1986 s. 536 Ikkevold

Rt. 1990 s. 607

Rt. 1991 s. 616 Hemmelig videoopptak

Rt. 1993 s. 300

Rt. 1996 s. 1401

Rt. 2001 s. 668 Hemmelig videoopptak II

Rt. 2001 s.1589 Raufossdommen

Rettens Gang

RG 1993 s. 77 (Brukerområde)

RG 1996 s. 1241 (konkurranseklausul)

RG 2002 s. 162 Hemmelig videoopptak III

Dommer fra arbeidsrettene

ARD 1918-1919 s. 233 (Stemplingsur)

ARD 1940 s. 17

ARD 1950 s. 16 (Stemplingsur)

ARD 1951 s. 201 (Personkontroll)

ARD 1958 s. 19 (Stemplingsur)

ARD 1959 s. 1 (Effektivitet)

ARD 1968 s. 44 (Stemplingsur)

ARD 1978 s. 110 (Stikkprøvekontroll)

A